Aalto University
School of Science
Degree Programme in Computer Science and Engineering

Ossi Ala-Peijari

Bitcoin The Virtual Currency:
Energy Efficient Mining of Bitcoins

Master's Thesis
Espoo, 24.08.2014

Supervisor: Professor Antti Ylä-Jääski, Aalto University
Advisor: Phd Miika Komu

Aalto University
School of Science
Degree Programme in Computer Science and Engineering

ABSTRACT OF
MASTER'S THESIS

Author: Ossi Ala-Peijari

Title:
Bitcoin The Virtual Currency: Energy Efficient Mining of Bitcoins

Date:	24.08.2014	**Pages:**	81
Major:	Data Communication Software	**Code:**	T-110
Supervisor:	Professor Antti Ylä-Jääski		
Advisor:	Phd Miika Komu		

Bitcoin is a distributed, virtual currency without centralized control. While a few services accept bitcoins directly, it is also possible to exchange bitcoins into fiat currency and vice versa.

Bitcoins are effectively computation puzzles that are mined based on a brute-force algorithm. As computation requires electricity, it can be stated that the miners are exchanging energy for bitcoins. However, electricity is not usually free and the energy efficiency of the mining devices can vary. Thus, some low-efficiency devices could be considered mainly as an environmental hazard because the expense of using the electricity exceeds the profits.

The miners are competing with each other to find solutions, which has resulted in an arms race to use specialized hardware for mining. While this improves energy efficiency, the computational limit for profitable Bitcoin mining is still a moving target. In this thesis, we study and analyse past developments in this limit and try to estimate its future directions.

Keywords: Bitcoin, Mining, Efficiency

Language: English

Aalto-yliopisto
Perustieteiden korkeakoulu
Tietotekniikan koulutusohjelma

DIPLOMITYÖN TIIVISTELMÄ

Tekijä:	Ossi Ala-Peijari		
Työn nimi:	Bitcoin virtuaali valuutta: Energiatehokas louhinta		
Päiväys:	24.08.2014	**Sivumäärä:**	81
Pääaine:	Tietoliikenneohjelmistot	**Koodi:**	T-110
Valvoja:	Professori Antti Ylä-Jääski		
Ohjaaja:	Phd Miika Komu		

Bitcoin on hajautettu kryptografinen virtuaalivaluutta vailla keskitettyä hallintaa. Toistaiseksi harvat kauppiaat ottavat suoraan vastaan bitcoineja, mutta bitcoinit voi muuttaa euroiksi tai eurot bitcoineiksi useassa bitcoin pörssissä.

Bitcoin perustuu tiivisteisiin ja laskennalliseen vaativuuteen löytää tiivistettä vastaava alkuperäinen numerosarja, joka onnistuu nykyisen tiedon mukaan vain ns. brute-force menetelmällä. Tämä vie merkittävän määrän energiaa ja voidaankin sanoa, että bitcoinien louhinta onkin sähkön vaihtoa bitcoineiksi. Sähkö ei luonnollisesti ole ilmaista ja sen hinta vaihtelee suuresti, kuten myös louhintalaitteiden energiatehokkuus. Tästä syystä energiatehottomat laitteet ovat haitaksi ympäristölle, koska niiden louhinta ei ole voitollista.

Bitcoin verkossa louhijat kilpailevat toisiaan vastaan etsimällä bitcoin verkon hyväksymää tiivistettä. Tämä on johtanut siihen, että louhijat ovat alkaneet ostamaan louhintaan erikoistuneita, energiatehokkaampia laitteita. Tämä taas on puolestaan nostanut energiataloudellisuuden vaatimusta, koska bitcoineja louhitaan entistä nopeammin. Olemme työssä analysoineet tätä vaatimusta ja yleisesti bitcoinin tulevaisuudennäkymiä.

Asiasanat:	Bitcoin, Louhinta
Kieli:	Englanti

Acknowledgements

I would like to thank Miika Komu, Matti Siekkinen, Jukka Nurminen, Andrey Lukuanenko, Jiang Dong, Jaakko Salo and Toni Ruottu for their input on this thesis. Special thanks for Andrew Geyls for supplying the hash rates for the mining data. Additionally, I would like to thank my parents Maija Ala-Peijari and Jukka Ala-Peijari for their support

Contents

Acronyms

FBI Federal Bureau of Investigation

NFC Near Field Communication

Mhash Mega hash

GPU Graphics Processing Unit

CPU Central Processing Unit

Ghash Giga hash

US United States

POSIX Portable Operating System Interface for uniX

SHA Secure Hash Algorithm

HDD Hard Disk Drive

SSD Solid State Drive

PPS Pay Per Share

PPLNS Pay Per Last N Shares

IRC Internet Relay Chat

DNS Domain Name System

NAT Network Address Translation

ASIC Application Specific Integrated Circuit

ARM Advanced RISC Machines

RISC Reduced Instruction Set Computer

FPGA Field-Programmable Gate Array

BFL Butterfly Labs

HIIT Helsinki Institute for Information Technology

TKK Tekninen Korkeakoulu (Helsinki University of Technology)

Chapter 1

Introduction

1.1 Motivation

Currency has made the transfer of value for goods and services easier for those who possess a similar understanding of the currency's value. As a consequence of its introduction, the earlier complicated system of trading goods has been replaced by a common medium of exchange that greatly facilitates trading of goods services.

The pioneer of the current fiat monetary system was probably a Swedish bank, [13] Stockholm Banco, that in 1657 started to issue paper currency to its customers, which was easily transferable and backed up by the promise of future payment in metals such as gold and silver. However, the bank issued more currency compared to the amount of mental it actually had in its reserves. This was probably the first time that people had a fiat currency in their hands because its value was not based on the actual metallic reserve that the bank had in their possession. This procedure is called fraction reserved banking. It started the beginning of the new monetary era, where banks did not need to possess the amount of currency or metal that customers had deposited, but only a fraction of it. The rest of it could be used to lend to other customers. This meant that the bank did not actually possess the amount of currency they claimed. In other words, the value the bank had promised customers was just a promise based on the fact that only an insignificant set of customers would normally demand their money on any given day.

Later, the bond between money and metals was broken and the value of money was determined in open market. Fiat currencies, however, are vulnerable to political market tampering by, for example central banks, which can by their decision increase moneys supply making existing money less

valuable. Also, political decisions can be taken to seize money as happened recently in Cyprus [15, 23], where large bank deposits over 100 000 euros were subject to bailout tax. These actions lower the confidence in the currency, which usually decreases in value as a result. Our current monetary system also has certain entities, otherwise known as central banks. These entities have the power to influence value of money, but they differ from country to another and in the numbers of people who are needed to make the key decisions. In Bitcoin, however, there are no such entities. The number of bitcoins available is increased by predetermined rules. Bitcoins cannot be seized from the users' Bitcoin wallets without their private key and also optionally a password. It is essentially a currency that no government or governments have a monopoly of control over. It is also easy to move. In the words of Wired article, "Bitcoin is a dollar bill, with a teleporter built in" [1]. However, the definition does not make reference to the inability of governments to control the currency.

In the New Yorker the creator(s) of Bitcoin, Satoshi Nakamoto, the pseudonymous person or group of people who designed and created the original Bitcoin software, was quoted in the New Yorker (as) saying, "The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve". The New Yorker argues that this is why Satoshi Nakamoto was politically motivated to create Bitcoin [8]. The article mentions that it is illegal in the US to adopt an own currency that competes with the US dollar and speculates that this was one of the reasons why a pseudonym was used for creator(s). From viewpoint of many people, the skill sets required to develop Bitcoin is vastly challenging and includes economics, cryptography, peer-to-peer networking and C++. This has raised innumerable questions and also possibly interest in Bitcoin as many have tried to find a way to cheat the network by finding errors in the Bitcoin code, but none of the current attacks have been against Bitcoin itself, but rather the system that it runs on top of.

The main difference between a fiat currency and Bitcoin is that instead of having institutes similar to central banks, there are only users following predefined rules and the majority of these rules should be followed because that would otherwise signify that Bitcoin has split into two different currencies. Based on the New Yorker article, Bitcoin could be defined as a trust currency [8]. In other words, users do not have to trust the creator of the currency be-

[1] Dan Kaminsky, Wired, 05 03 2013 `http://www.wired.com/opinion/2013/05/lets-cut-through-the-bitcoin-hype/`

cause the rules and code are there for all to access. This transparency is also present in transactions, which implies that every transaction is public. The entity that could be the best candidate for exercising control over Bitcoin are the client developers, because they implement the rules, but changes must be unanimous among the developers and not conflict with previous rules.

1.2 Scope of the Thesis

The actual contributions of this thesis consist of providing a formula to calculate the expected profit and income for Bitcoin mining, and estimate how many miners are actually making a profit out of mining. We also tested some of the devices ourselves to ensure results were unbiased in estimating the actual hash rate of the device and their energy consumption, against which profit and energy consumption estimations can be made. The hash rate refers to the rate at which a device can squeeze information out of the block to a hash. A higher hash speed results in a higher chance of successfully mining bitcoins.

We do not dive any further into economic history. Brief history of money is given in Surowiecki's article [41]. Nor do we proceed deeply into the legality of the use of bitcoins as a currency. For the interested reader a short article on the subject has been written by Edwin Jacobs [16], and additionally some problems has been addressed in a New Yorker article [8]. Bitcoin is a politically interesting subject as, for example, in the US competing currencies are illegal [22]. Some articles argue that Bitcoin is not illegal because it is not real money[33] [2], but a deeper legal analysis is scoped out of the thesis. However, we will go into some detail regarding to the Bitcoin protocol and offer an overview of how Bitcoin is structured, and how users are able to contact each other in the Bitcoin network.

Our main focus is Bitcoin mining and, to study when it is profitable. The data that is used in the analysis is mainly from our own tests, but also some results from" Tomshardware" tests will be referenced [38]. There are some efficiency numbers found in Bitcoin Wiki, but according to some documents [31] it might be somewhat biased. Fortunately, miner called Andrew Geyls has provided us data of user accounts from mining pools, based on which we try to estimate how many people could be losing money while mining

[2] Richard W. Rahn Washington Times 28.5.2013 http://www.cato.org/publications/commentary/preserving-their-monopoly-monopoly-money?utm_source=Cato+Institute+Emails&utm_campaign=99e8687f97-Cato_Today&utm_medium=email&utm_term=0_395878584c-99e8687f97-142439457&mc_cid=99e8687f97&mc_eid=9d7eb3430e

bitcoins. We will not discuss any additional technology regarding Bitcoin, such as bitcoin usage with NFC [5], but one security related device that increases security will be mentioned later.

The main focus is on the energy efficiency of Bitcoin mining. A secondary question we try to answer is how the network reaches consensus.

1.3 Structure of the Thesis

We will describe the bitcoin service in background chapter. This chapter describes how Bitcoin is structured, e.g. how transactions are stored for everyone to read. In the next chapter, Entities in the Bitcoin network, we discuss the miners and the clients. Both are essential for Bitcoin to work. Miners is a person or software that tries acquire bitcoins by mining. We use term "clients" when we are talking bitcoin wallet software or bitcoin mining software.

As in other peer to peer software, the clients need to install the software, which is explained in the third chapter along with clients and some of the entities involved in maintaining and running bitcoin. Client types are web-based and local software-based clients.

Additionally to clients, who are users of bitcoins, also miners are required to perform tasks in the network of which they get rewards when they find acceptable solution first. Miners are required to be connected to the client either directly or indirectly. An indirect example is pooled mining, also explained in this same third chapter. Similarly solo mining is explained, which is the direct approach. We will also describe the pool reward algorithms and offer an explanation of why miners are necessary to the Bitcoin network.

The fourth chapter, Communication in the Bitcoin Network, we will explain how datagrams are transmitted through the Bitcoin network, and also describe each channel. Additionally, this chapter explains what occurs if clients do not reach a consensus on rules.

Next, we explain in the fifth chapter what is the contribution of the thesis to the Bitcoin research concerning energy-efficient mining. Bitcoin Wiki includes some results but, some information is not always accurate as some of the results have been done with over-clocked devices, even though Bitcoin Wiki does not always clearly show this [31]. The fifth chapter also describes the current state of mining. There are a few different classes of devices used for mining. In this chapter, we shows the different hash rate distribution of users. In this thesis, we consider user to be person who pays with bitcoins.

This is followed by the sixth chapter, where we test and analyse the

devices, describe the results of the test analysis, and estimate the profitability of the different devices. Our main aim is to understand what is the most energy efficient way of mining.

The seventh chapter contains further discussion concerning the results of the test, and what is the possible impact of the direction that mining seems to be taking.

In the concluding chapter of this thesis, we will discuss the areas that require more research, as there seem to be some gaps not covered by research papers and are only available at bitcoin wiki. Finally, our findings are summarized and conclusions drawn at the end of this chapter.

Chapter 2

Background

Bitcoin is a cryptographic currency which allows users to transfer money over the Internet as easily as sending email. As the Wired article [19] describes it, "bitcoin is a dollar that has a teleporter wrapped around it". However, the ease with which money can be transferred raises some concerns. The FBI defines bitcoin with the lower case as being the currency while Bitcoin with the upper case refers official protocol and software called Bitcoin [31]. This rule will also be followed in this manuscript.

In Bitcoin, an important requirement is that each client node connected to the Bitcoin network has a copy of the Bitcoin ledger called a block chain that consists of all transactions of the Bitcoin network. This implies that no centralized authority exists and transactions are distributed, verified and validated by Bitcoin users [32]. This requires a structured way of handling each transaction and keeping track of the transactions that have been verified. For this reason, so called blocks exist in Bitcoin that contain verified transactions. When the blocks have been accepted by the user, they are stored in the user's block chain and distributed to every other users' block chain as well. In this chapter we will have a look at the details of transactions, blocks and the block chain.

Bitcoin is structured according to different functionality. In this section, we explain the different structures from smallest to largest. The smallest one is a transaction that holds information regarding a transaction, but similarly to a block, it is linked back to the previous transaction, thus forming a one-way linked list of transactions. Blocks, on the other hand, contain multiple transactions and when a block is accepted by Bitcoin users, it is considered to be part of a block chain. Similarly to transactions, blocks in a block chain form a one-way linked list of blocks. This is illustrated in Figure 2.1

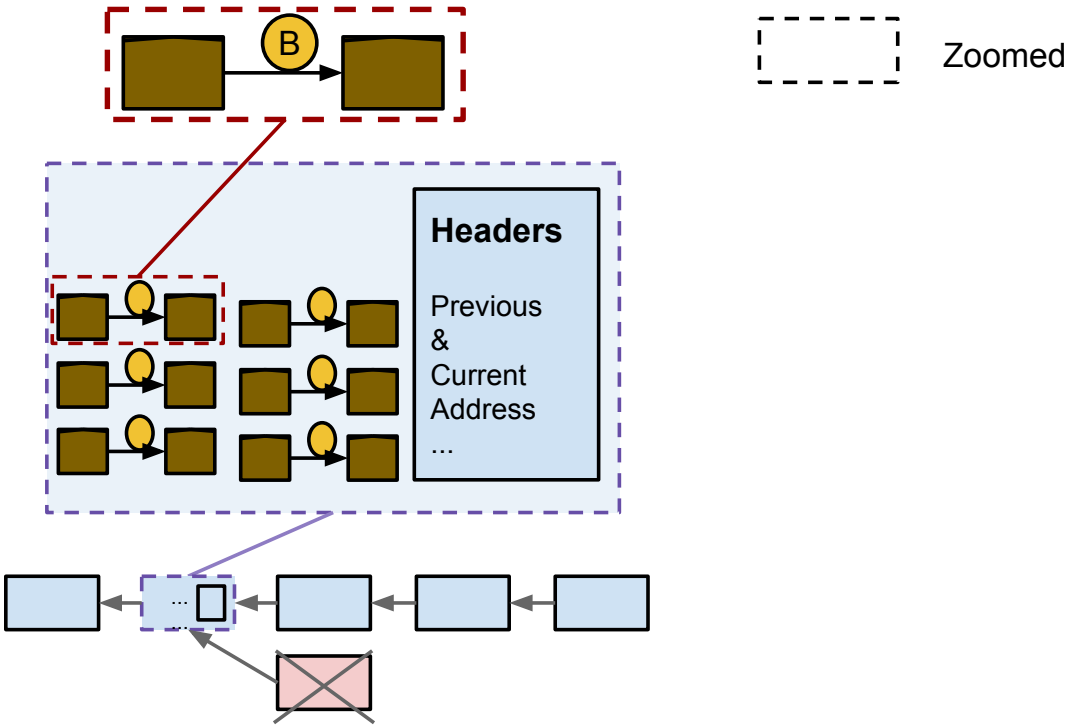

Figure 2.1: Structure of Bitcoin

2.1 Transaction

A basic transaction is defined as an event where a user transfers money to another user. However, this procedure in bitcoin is somewhat less obvious. Bitcoin includes no traditional bank account stored in a relational database with a balance field. Instead, so called a ledger called the block chain defines each transaction in the Bitcoin network.

A user has a private key acting as a password to the transaction output, which the user can use in future transactions as inputs. A public address refers essentially to a public key that is part of the corresponding private key and acts as an "account number". Thus, Bitcoin is not based on accounts authorized by username-password pairs, but rather public-private key pairs.

Transaction chaining has been explained in "zero-cash" paper [26], which illustrates the flows from one transaction to another. In brief, transaction itself is a container that has a output attribute to define the number of bitcoins a user has access to, and thus, combining all user transaction outputs and inputs reveals user's bitcoin balance. Transaction inputs are sums of earlier transactions in the sense that, each transaction generates one or two

new outputs, depending on whether the exact number of bitcoins can be gathered from previous bitcoin transaction outputs. However, a transaction can "consume" multiple outputs but they can only be used once and as a whole which is why transaction might have second output as a loop-back to assign some of the bitcoins back to sender.

As an example, only one output would be created when the exact amount can be combined for the payment from previous transaction outputs. However, in most cases two outputs are generated. So the first output is accessible to the receiver of the transaction and the other is the number of bitcoins that were not meant to be spent on the transaction, but were required to acquire an adequate number of bitcoins for payment, therefore, second output is created for sender to use in future transactions.

As it is also very likely that at some point, a user has multiple smaller transactions, but not a single one that is high enough to pay what is a sufficient amount, one of the Bitcoin's features is that users are allowed to combine transactions. Clients take previous transactions as bitcoin inputs, which would be the same as combining multiple real world bills to pay for something that is worth more than a single bill. The difference with a fiat currency is that the Bitcoin has no standard bill value which each bitcoin transaction should hold. As another analogue to the real world, Bitcoin output corresponds to both a payment to a cashier, who charges the required amount, and the change that is returned to a customer.

If a user pays with a credit card, the store owner has to pay some percentage out of the transaction. In the Bitcoin world, users did not need to pay a transaction reward on transactions with a low number of required inputs prior to 2013, but, if they did, the transfer was usually processed faster [4]. This reward is marked so that it is neither in the seller's or buyer's output, and is considered as part of the reward for a miner who generates an acceptable proof of work that allows the block containing the transaction to be part of the block chain. In the following figure, the most common transactions are illustrated.

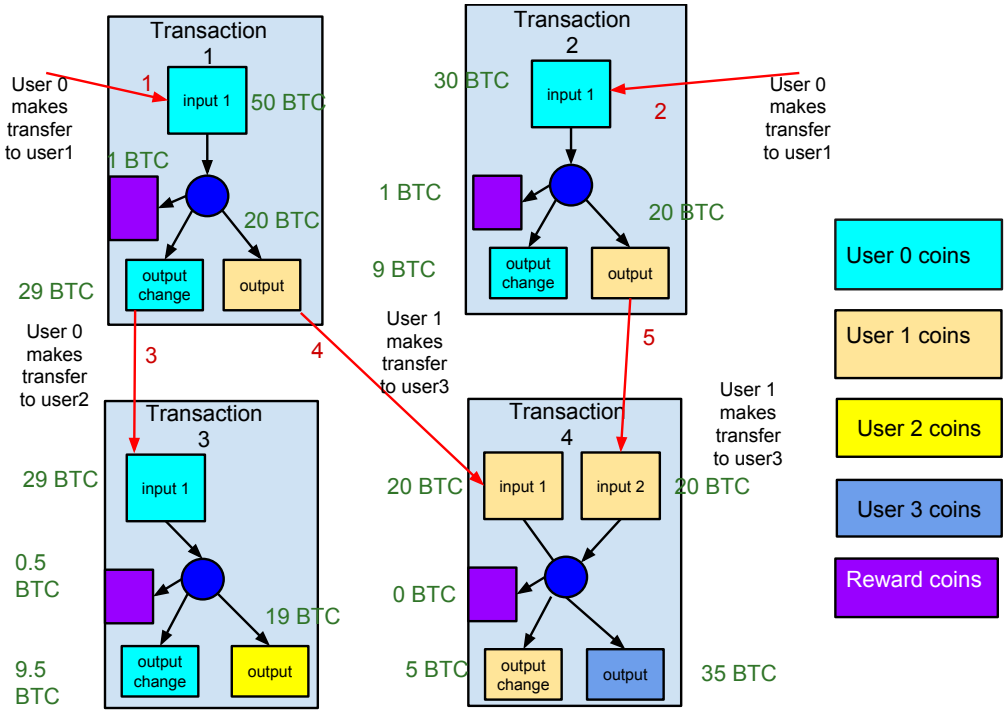

Figure 2.2: Transaction flow

A simple case of transaction is shown in the upper left in Figure 2.2. In this case, a user 1 transfers bitcoins to another user 2. In transaction 1, the Bitcoin client takes the output of previous transaction as the input that is indicated by the red arrow and number 1. The end result of this example transaction is that the user sends more money than the user wanted to spend. This means wallet creates a "change" output that is accessible to user 0, while a second output is accessible to the receiving user 1. User 0 who sends money in transaction 1 also gives a transaction reward of 1 bitcoin to a user x, known as the miner, whose task is to generate acceptable block that gets validated. Reward is received after the block has been validated. Reward has been illustrated as "Reward coins" in Figure 2.2. From a technical point of view, the transaction reward is the value that has not been assigned to any outputs. It is calculated from what is left over from the inputs when the outputs have been deducted from inputs.

Traditional transactions generates two outputs similarly to transaction number 1. One output is available to the user who sent the money, which could be considered as a change. The second output is assigned to the user who was actually supposed to receive bitcoins.

In the bottom left transaction at 3, user 0 is shown reusing the money he or she received as change from transaction 1. This is indicated by red

arrow number 3. Bitcoins can be divided by up to eight decimals, but for readability it is not shown in Figure 2.2.

At the bottom right, transaction 4 shows user 1 combining transaction 1 and transaction 2 outputs to pay user 3 a sufficient amount. In the same transaction, red arrow 4 indicates user 1 using bitcoins he or she received in transaction 1 from user 0, and red arrow 5 the output received from a different transaction from the same user 0. The combined value of these outputs is 40 bitcoins, which is a sufficient to pay 35 bitcoins. The remaining 5 bitcoins is left as change for user 1 and the payment of 35 bitcoins is accessible to user 3.

Transaction 4 also illustrates that no verification reward is necessary. However, without a verification reward, the miner i.e. user x prioritizes transactions with a higher reward. As combining numerous transactions requires miner to check validity of each output the miner might prefer transactions with fewer combined outputs or higher transaction reward. For readability reasons, Figure 2.2 shows only two combining outputs, but a larger number of outputs can be used.

In Bitcoin, transactions form a one-way linked list that allows tracing previous accounts that a bitcoin has been associated with. Related to this, one could argue that Bitcoin merely offers tools for privacy, and, essentially, privacy in Bitcoin depends on the user's own actions. If the person is known by some people, then they can trace his or her transactions and calculate the balance of the account [17]. Users can, however, hide behind the pseudonymity of a public account address[28, 39]. What this means is that the real identity cannot be established even when the account number is known. Bitcoin services exist that allow the users to hide their tracks by exchanging bitcoins for different ones.

It is impossible to use non-existing coins because of the trail checks bitcoin networks does for each transactions. Bitcoin-protocol always requires the Bitcoin network to accept a transaction, and a user who initiates the transaction has to cryptographically sign the transaction and the Bitcoin network will validate it [1]. The account of the user is authorized by a private key, and the corresponding public key is known to the network, and acts as a pseudonym [24]. When a user transfers bitcoins, he or she includes previous transactions as input and defines the amount he or she wishes to send. One output consists of the address the sender sent bitcoins to, and possible second output consists of the change that was left over to be "returned" to the sender. Then, the transaction is signed by the sender with his or her private

[1] Zulfikar Ramzan, Khan Academy, 1.8.2013 `https://www.youtube.com/watch?v=9-9_v1wSPBQ`

key [2]. From the signed transaction, everyone can verify that the transaction is valid using the public key of the sender.

Signing transactions, however, does not prevent users from double spending their bitcoins. Double spending is essentially using same bitcoins twice and to prevent it, Satoshi Nakamoto came up with a block-based validation where double spending is prevented by allowing only one block, containing multiple transactions, to be validated at a time [27]. This prevents double spending because the miner checks the balance and only one transaction from the account can be approved to avoid the problems that would arise from having multiple entities concurrently checking transactions. A form of double spending is only possible in transactions that do not wait for the block to be added to the block chain, as was described in an article on Financial Crytography by Barber et al. [40]. Even then, there will not be any additional bitcoins because one of the transactions gets denied. Consequently, Bitcoin avoids double spending when the Bitcoin protocol is used as intended. Double spending prevention is based on the transaction chaining, and the validation procedure.

One transaction feature exists that might be useful but it is not used. Bitcoin allows conditional transactions [40]. One example of this was defined in Bitcoin Wiki [3]: On the Wikipedia site, or some other site heavily dependant on the users' contributions, users could deposit funds to earn trust. This allows the site to be confident that the user is not a bot trying to create a huge number of accounts, but it also discourages real users from possessing multiple accounts. The concept is based on a user depositing funds, which are then released in a predetermined time frame. This deposit will not be accessible to the site owners, and its only function is to prevent the user using the bitcoins he or she has deposited. In other words, this means that funds are held captive in the Bitcoin network until the determined time has passed. When the time has elapsed, Bitcoin network automatically released bitcoins back to the user.

2.2 Blocks

A block is a containers of bitcoin transactions, and the transaction is verified by a miner who submits the valid block to the Bitcoin network. When a bitcoin user's bitcoin client validates a block, it is added to the user's

[2] Zulfikar Ramzan, Khan Academy, 1.8.2013 `https://www.youtube.com/watch?v=9-9_v1wSPBQ`

[3] Bitcoin Wiki, 20.12.2014 `https://en.bitcoin.it/wiki/Contracts#Example_1:_Providing_a_deposit`

personal block chain on top of the last block considered valid. The more blocks that are validated, the less likely it is for the block to be replaced by another competing block. This means that the transaction ends up being the building block in a block chain [32], and to replace the block, the following blocks need to be replaced with ones that on average take longer time to mine.

Mining of blocks should be considered a competition where every miner tries to find a hash value on a agreed range. This range is determined by a difficulty attribute that is adjusted by each miner every 2016 blocks in order for the winning hash to be found by miners on the average every 10 minutes. As these hashes are unpredictable, anyone could find a hash on the first try or it might take hours.

Mining could be thought as a reverse lottery where players i.e. the miners have devices generating the numbers, and the right number sequence for the lottery is known. However, different devices have different computational capabilities and can generate solutions faster than others.

Winning the highest amount in the Finnish lottery requires seven correct numbers. However, in Bitcoin mining, only one winner exists for every round and the difficulty dictates the total number of right numbers that are required in order to win the so-called block reward. A block reward consists of the transaction rewards of each transaction in a block described in the Section 2.1.1 as well as the network reward and both are given to miner of the block. So the total reward is combination of network reward and transactions reward that is collected from transactions included in the block paid by the ones sending bitcoins in bitcoin network.

The Bitcoin network's reward is halved approximately every 4 years. It started at 50 BTC and is currently 25 BTC. While the network reward decreases, the cumulative transaction rewards, resulting from each partitioning of the total reward, will continue to grow ever larger as more and more transactions are verified by miners, assuming that more users start to use bitcoins. While the increase in transaction rewards is not expected to cover the reduction of network rewards to miners, it is hoped it will lead to deflation, which could bring new users to the Bitcoin system and reward existing users.

Bitcoin has not yet been of interest to larger businesses such as Amazon. The company introduced their own electronic currency, which currently seems to be centralized and only available for US customers.

The purpose of the block is to verify transactions and to reward a miner who has generated an acceptable proof of work. The miner generates a proof of work by hashing the block header consisting of the following attributes: Version, which is the version of Bitcoin; hashPrevBlock is the hash of the previous block; hashMerkleRoot is the hash generated from the Merkle tree

of transactions; Time, which is the Unix or POSIX timestamp indicating current time; Bits indicates the current difficulty that changes every 2016 blocks; Nonce, finally, is a running value that is incremented by the mining client every time the block header [12] is hashed.

2.3 Block chain

The Block chain is a chain of blocks, which could be described as an open ledger of all the Bitcoin transactions. As a rule, a valid block chain has always the same genesis block, which is the first block in the chain and the other chains are ignored by the network nodes [4], which are the Bitcoin clients connected to the Bitcoin network. A chain can include multiple different branches, but eventually the network forgets these other branches. This is handled by the Bitcoin nodes that filter blocks that they think do not comply with the network rules. Blocks complying with the network rules form a chain that is effectively a one-way linked list.

Mining of blocks could be considered as a competition. When competition is tight, multiple valid solutions are found, but only one miner can have the reward. These valid blocks, but left out from block chain will become invalid blocks and branches. It is said in Bitcoin Wiki [5] that the branch with greater combined difficulty is chosen for the block chain that is the sum of the blocks difficulties in the branch. The bitcoin network, however, sometimes chooses block with a lower difficulty over the higher one. The reason for this is the previously mentioned "greater combined difficulty" rule. A block found earlier has miners already generating the following block for it. Therefore, the block mined earlier is more likely to receive the next block. The combined difficulty rule forces bitcoin network to accept a branch that has a higher combined difficulty, which could include some blocks with lower difficulty compared to another branch that was ignored earlier.

The block chain is a one-way linked list because each block contains the address of the previous block. The block has a field for only one previous block address. This means that multiple valid branches cannot exist in the bitcoin network, but some invalid branches might turn into valid branches when they reach a higher combined difficulty. The block's hash is generated from the block's attributes and compared with the current difficulty value in hexadecimal form. A hash with more zeroes in front of the value is considered to be more difficult to generate, and thus has a higher difficulty.

[4] Github, 20.12.2013 `https://github.com/bitcoin/bitcoin/blob/b86ed6ff23fbc5a71587648c5ae547ad404e09f2/src/init.cpp`

[5] Bitcoin Wiki, 20.12.2013 `https://en.bitcoin.it/wiki/Block_chain`

As a result of the chaining, a block chain is nearly impossible to alter since changing one block would mean that someone trying to change a block would need to generate a branch with a higher combined difficulty value than the original. The bitcoin network also enforce a rule where the first block must be the genesis block generated by Satoshi. This prevents the malign mining community from replacing the whole block chain.

The block chain is a very important concept for the Bitcoin network because all Bitcoin users, as well as miners, must rely on its data. Integrity is very important, but due to the peer-to-peer nature of Bitcoin it includes some compromises. One of the compromises is that the latest block and its transactions added to the block chain cannot be fully trusted because it could be replaced with another block or branch. Consequently, not only might every bitcoin user have to wait on average 10 minutes window for the miners to be able to add their transaction to the block, but bitcoin allows other users to validate the block and even generate additional blocks to reinforce the block's position in the block chain. For example, the Bitcoin network has faced an incident in the past where earlier Bitcoin clients did not accept a new block because the block's size in kb was larger than the earlier Bitcoin network rules allowed it to be. To solve this problem, the protocol version was changed to follow the old rules [18]. This can occur more frequently on a smaller scale, and the higher the number of confirmations, the higher is the probability that these blocks and transactions stay in the block chain. It seems that there exists no guidelines on how many blocks should be expected, and different merchants expect different numbers of blocks. Some of them do not even require a single block to be validated.

The block chain is open and anyone can browse the block chain, using a web browser from `http://blockchain.info` or `https://blockexplorer.com`. [4]. All users of bitcoins have a pseudonym, which is their public address and functions as public key. If an eavesdropper is able to form a connection between the user's real identity and his or her public address, then the eavesdropper can identify the user's balance and see the transaction history from the block chain. Bitcoin users can, however, creates new addresses to limit their exposure. This has also been discussed in "Bitcoin is not PRISM-proof" by Neagle [29]. Bitcoin by itself does not provide full privacy.

Chapter 3

Entities in Bitcoin Network

The previous chapter explained the structure Bitcoin. This chapter describes the entities of the Bitcoin network, which consists of two main entities called clients and miners. Miners could be thought as a subset of clients because they, at least indirectly, need to be connected to a Bitcoin client to receive transaction and block information. Network nodes validate transactions and spread transactions further to network. Thus, it can be argued that network nodes are distributors. Miners, on the other hand, usually verify a large number of transactions during their proof of work generation.

Network node is essentially the an entity that is connected to the Bitcoin network. It can be a software client or the backend process of a web-based client that is connected to the Bitcoin network.

This chapter defines what are web-based clients and software-based clients. The official Bitcoin client wallet is not the only the only wallet that exists. Multiple wallets exists, but to function in a Bitcoin network, they have to have similar rules to the official client. Previously, miner client was included in the official Bitcoin wallet. Currently, it seems that no official miner client exists. Multiple unofficial ones exists and no one-size-fits-all seems to exist.

3.1 Clients

Multiple clients exist for user, but, alternatively, they can create their own. From a developer's viewpoint, there are a few things should be brought up. Bitcoin has test beds called test nets that can be used to test the functionality of Bitcoin clients without using any bitcoins. Therefore, to some extent, it could be argued that the bitcoin is a somewhat developer-friendly currency. Multiple Bitcoin wallet clients are available, probably due to availability of test beds. It could be argued that clients also make bitcoin more of a

currency than software because users gives his vote to rule-set implemented by the developer. Developer might for example decline to transmit someone's transactions in the bitcoin network, which might slow these transactions process time.

Two types of client classes exists. The most obvious is the software client. Such clients are vulnerable to different kinds of malware viruses that could steal the wallet's private key and steal funds from the user. Web-based clients, on the other hand, place huge trust in third parties. Neither is an ideal solution at the moment. However, there are some interesting projects under work that would prevent malicious users from stealing funds from a wallet, such as Trezor. [1].

3.1.1 Web-Based Clients

Web-based clients basically work in the same way as online banks and many exchange services that trade bitcoins for the fiat currency of the user's choice, might consider offering web-based wallet service in the future. Such services store the private key of the user on their servers and offer an interface for users to manage their transactions.

Bitcoin is new, and, thus, most web-based service providers do not have the same level of security as a traditional bank. There has been several incidents where a web service has been compromised and an attacker has acquired the keys needed to steal user's bitcoins.

The benefits of having a web-based service is that the user does not need to worry about malware stealing his unencrypted private key from a device as it is by default. Because the software clients participate in Bitcoin transaction and block distribution, web-based client user saves bandwidth and disk space. Time is also saved in some situations when the transaction process requires the user to have the latest block. If the user has not kept his Bitcoin client open for several days, it might take some time to download missing blocks from the network. Thus, when the user installs the software client it might takes hours to download all the blocks. On the other hand, a web-based client service provider keeps constant track of the blocks in any case and only needs to store one copy of the block chain to servers, which is cheaper than having every user redundantly store the block chain in their devices.

[1] Bitcoin Trezor, 7.7.2013 `http://www.bitcointrezor.com/?ref=pool`

3.1.2 Software Clients

Software clients are a type of software installed on user's devices that interacts with the Bitcoin network and is required to store the whole block chain. In order to work properly, it has to distribute transactions and blocks to other bitcoin network nodes (i.e. wallets) and receive what others have found.

A software client reads the transaction data from the block chain, which holds all the accepted blocks and transactions. To create a transaction, the client has to decide which previous transactions it consumes to create the next transaction as the transaction output can only be used once. The client then signs the transaction previously signed by someone else with its own private key and addresses it to the public key or IP-address of the user receiving the bitcoins.

Storing of the said private key is currently a weak point of the official Bitcoin and other Bitcoin clients. The last time it we tested in the end of 2012 the private key was not protected by encryption. Essentially, it is only a plaintext file that can be copied and deleted. Therefore, it is easy for a malicious actor to steal the private key file and steal bitcoins signed with the key, which is the only thing that tells the network that the user owns the coins. Trezor [2] is probably a concept that will change this because it stores the private key on a physical device. It is designed only to sign transactions passed to the device and the device sends the end result back to the device, which sends it to the Bitcoin network to be validated and verified. In Trezor, the private key is never introduced to the device connected to the Internet and, thus, it becomes very difficult for a malicious user to steal the private key.

Another problem with software clients is still the rate at which the block chain is growing. At the end of the 2012, it was over 2.5gb. While it is a small amount on a traditional HDD, it might become a problem in a smaller SSD, and even more so with smart phones. A size of 2.5GB is not that large if the four years of operating time of bitcoin is is taken into consideration. However, the rate, at which the block chain has recently grown, should be considered of sufficient concern for users to store it on their computers or smart phones. In 2013, the official client required every block to be stored on the HDD until it allowed the user to create transactions for at least two reasons. First is that software client needs to know which bitcoins have been used. User trying to use bitcoins twice would only be noticed by the bitcoin network nodes, which would not transmit the transaction any further. Also, the Bitcoin clients need to know all of the previous transactions when user has

[2] Bitcoin Trezor, 7.7.2013 `http://www.bitcointrezor.com/?ref=pool`

received new transactions, because this would alter the amount of bitcoins at the user's disposal.

3.2 Miners

Decentralization makes prevention of double spending difficult. The Bitcoin solution for checking double spending is to obligate each node connected to the network to check the validity of transactions. The miner receives transactions from bitcoin network node, which could be users own bitcoin wallet, verifies these transactions and provides a proof of work based on it, and the nodes then validate it. Double spending is prevented by the fact that only one proof of work solution is allowed to exist at a time, and by checking the validity of transactions in the generation phase of each proof of work. Basically, this means that the bitcoins used in the newly added block will also be available in the old block chain. At the same time, the proof of work verification and validation solves the double spending problem, and produces a predictable increase of bitcoins in the Bitcoin network.

There are two ways to mine. One is to mine alone, which is called solo mining. The alternative to it is called pooled mining. Pooled mining is similar to the concept of buying a lottery ticket for a group, where the winnings are divided fairly between the group members. The main reason for pools to exist was that the chances of slower miners receiving rewards became smaller when more people started mining. With poor luck, even faster miners could mine for months or even years without receiving any reward. The intention of pooled mining is, to at least, to flatten out the statistical anomalies by having more miners search for an acceptable solution to the same problem. When a group finds a solution, the pool rewards the users based on their contribution in finding the solution.

3.2.1 Mining and Merkle Tree

Mining has two major functions for the Bitcoin network. From the bitcoin user's viewpoint, the more important one is transaction verification and validation. This is also the way new bitcoins are introduced to the network because bitcoins are given as a reward for the one miner who finds the next block to included in the block chain. During mining, the miner calculates by itself the current difficulty level as shown in Figure 3.1 in step 1 as no centralized database exists in the Bitcoin network. Therefore, miners and clients need to have a common understanding of the current difficulty level, which all the network nodes recalculate after every 2016 blocks so they know

if new block they receive has acceptable difficulty. Miners also calculate difficulty. The increase or decrease of difficulty depends on the time it takes to generate 2016 blocks. Bitcoin network adjust difficult to compensate for the rise or decrease of the hash rate so that miners are able to find a new block on average every 10 minutes. When a miner begins mining, it has to have access to the block chain in order to determine the current difficulty level as illustrated in the first step shown in Figure 3.1.

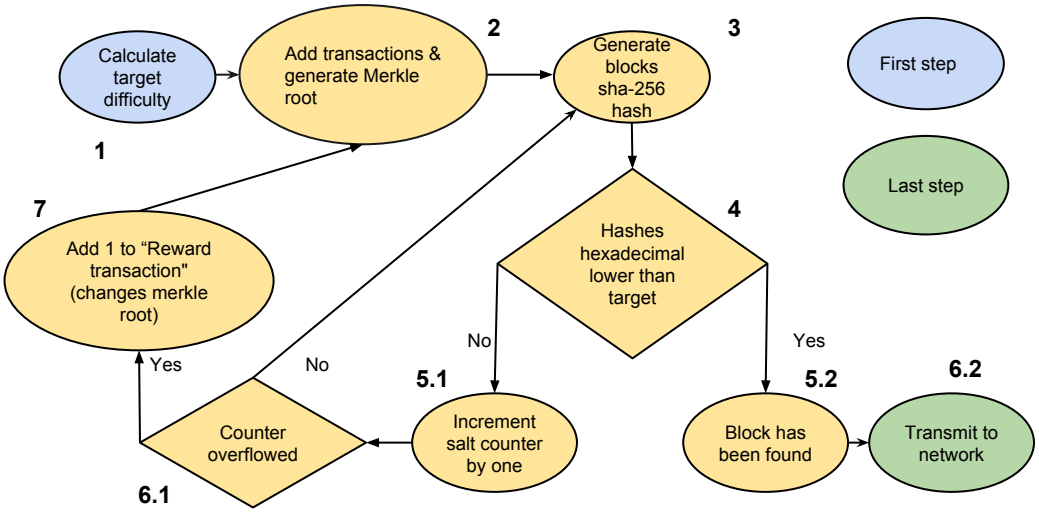

Figure 3.1: Mining illustrated

In step 2, the miner gathers the transactions and the previous block's hash value as well as other header values as shown in Figure 3.1. Then, Miner needs to generate the Merkle root. Miner constructs it by generating the Merkle tree [25] [3]. In the Merkle tree, the leaves have the transactions hashed with double sha256 hash, as shown in Figure 3.2.

[3]Wikipedia,10.9.2013 `https://en.wikipedia.org/wiki/Merkle_tree`

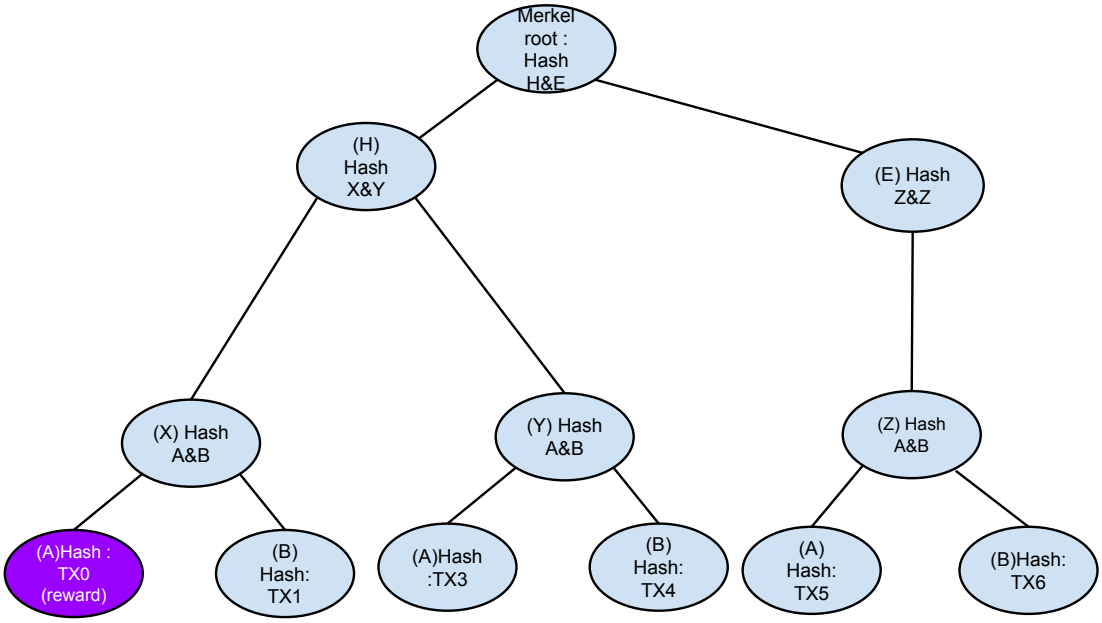

Figure 3.2: A Merkle tree with double hashing operation

The first leaf in Figure 3.2 contains the data that includes the reward transaction, which bitcoin network pays to the miner, and, as such, could be considered "special transaction". The reward transaction is marked as with violet in Figure 3.2. This transaction leaf will also have its overflow value, which miner increases every time nonce value has overflowed. This changes the Merkle root's value, which is important for the block's hash value. The Mining algorithm uses double sha256 for two of the siblings to generate the parent node. At the beginning, the tree has only leaves. The parent nodes of the leaves must be generated by combining both of the children of the parent node in order to generate a double sha256 from the hashes. When the tree does not have two siblings, Miner combines the last double hash with same hash value as shown in Figure 3.2. Miner combines both of the children to generate parent nodes until the root's value is obtained, which is called The Merkle root. The miners can choose the transactions they want, but Bitcoin rules restrict the number of transactions. One such rule is the maximum block size in kilobytes, as defined in the Bitcoin protocol.

The next step for the miner is to generate the block's own hash from the header values as illustrated in Figure 3.1, step 3. When the hash is generated, miner compares the hexadecimal representation of the hash with the current difficulty level. The difficulty level dictates how many zeroes must precede any other value in the block's hash for it to be acceptable [4]. Miner compares

[4]001 for example has higher difficulty than 011 because it has two zeroes instead of 1

the difficulty at Figure 3.1, step 4. If difficulty is high enough, block is considered to be a valid block and it will be distributed to the network as illustrated in steps 5.2 and 6.2 in Figure 3.1. If the network accepts the block, the miner receives the reward from the bitcoin network into his or her Bitcoin account[5].

When miner finds a block at the same time as another miner, the bitcoin networks chooses branch with the higher difficulty. The miner should not have the same block hash value multiple times as a result because some of the variables, such as unix time, will change, but also an mining client overflow counter is incremented each time a newly generated block hash does not have sufficient difficulty as illustrated in Figure 3.1, step 5.1. The overflow counter has only a few bits of space and, thus, will overflow frequently. When this occurs, mining client increments overflow value by one in the reward transaction, which is the special violet transaction seen in Figure 3.2 and illustrated in the mining phase in Figure 3.1, step 7. This will also change the Merkle root as even a single change will unpredictably change block's hash. Then the cycle starts again, whereby mining client might add transactions, which would require mining client to reconstruct Merkle tree. During step 6, if the counter does not overflow, the counter changes the block's hash sufficiently enough for the miner to be able to generate a new block with a new hash until the counter overflows again. It could be argued that steps 3,4.5.1 and 6.1 form an inner loop within the mining loop. Implementations can differ, but the miners should acknowledge if someone has found a new block, break the loop and start a new mining loop to build on top of the newly discovered block and not compete with existing ones.

3.2.1.1 Solo and Pool Mining

Two different types of mining exists. The most obvious way is to try to find a block alone, but with the increasing hash speed of the network, it is becoming less likely and more expensive for one miner to find a block unless the miner makes a significant investment in mining hardware. The miners' likelihood of finding a block is the same as the miners' hash rate divided by the network's hash rate:

$$\frac{OwnHashrate}{NetworkHashrate} \tag{3.1}$$

This means that if there were only 52 560 miners with the same hash rate, every miner on average should be able to find one block each year. This can

[5]Network reaches consensus to include the block to block chain, and, because block informs everyone that the miner has been given blocks reward it can be argued to be given by the bitcoin network

be calculated from the fact that network tries to balance its difficulty in such a way that a block is found on average every 10 minutes [6]. As an analogy people play lottery and similar games where they rely on their luck. From this perspective, mining could be argued to resemble gambling.

The Merkle root is different for everyone because the first transaction includes the miner's own address, and, thus, everyone has a different starting point. This ensures that the fastest machine on the network cannot monopolize all the rewards. For instance, someone might find an acceptable hash on the first try of the loop as described in the previous section, while someone else has to generate millions of hashes to find an acceptable one.

Marek Palatinus, usually known by his nickname "Slush", proposed that miners should get organized in order to acquire a steady reward stream instead of a few big pots a year. He founded the first Bitcoin mining pool on 27.11.2010, [7].

What follows is based on our experience of the pools as most pools do not distribute their code[8]. Pools assign each miner a subset of the hash space to check. A description is found at the Stack exchange[9] and, in some way, in Palatinuses' own stratum protocol [10]. From both we could make conclusion that the pools are used to deliver everything that is needed to generate the hash, and the only thing the miner has to do is to add a "salt", which is the nonce value until it overflows. Miners task is essentially to execute the inner loop mentioned earlier in this chapter and shown in Figure 3.1, but instead of reporting to bitcoin network, found blocks are reported to pool. This method meant that pool chose the transactions that were about to be added to block that pool was working on and, thus, validated. It can be noted that pool can prioritize rewards for its users over other transaction.

Now that the miners have become faster, they are also allowed to change the reward transaction. This allows them to take a larger hash range. Some pools also allow miners to change the difficulty level that determines which results or "shares" are reported. For example, miner could choose to send results with difficulty of 3 preceding zeroes in hexadecimal hash. In this case 00010.. would be reported, but 00100... not. However, if miner chose to report with two zero difficulty he would report both, but get smaller reward

[6]There are 52560 * 10 minutes in a year 60*24*365/10

[7] Bitcoin Wiki, 20.12.2013 `https://en.bitcoin.it/wiki/Comparison_of_mining_pools`

[8]Pushpool seems to be exception, but lacks some parts like web GUI `https://github.com/jgarzik/pushpool`

[9]StackExchange,27.8.2013 `http://bitcoin.stackexchange.com/questions/12955/how-do-mining-pools-distribute-work-effectively`

[10]Mining Bitcoin CZ 10.10.2013 `https://mining.bitcoin.cz/stratum-mining`

per reported result. Both help the pool and the individual miner because less bandwidth is needed to communicate between pool and the miner client.

A share in a pool is an acceptable block hash. The difference between the acceptable block hash of pool mining and the acceptable block hash of solo mining is that in pools an acceptable pool hash is easier to find. It naturally depends on luck and hardware, but, with a GPU, an acceptable pool hash is found every few seconds as we measured. In contrast, finding an acceptable block hash might take a year or even years during the latter half of 2012 .

It is reasonable to assume that the pools check that miners actually generate every hash in the hash space provided by the pool, and do not cheat by, for example, checking every second hash of the block. Cheating has been prevented by giving the miner a reward based on the previously mentioned shares. The transaction reward address is assigned for the address of a pool so that nobody can hijack the reward from the pool. Finding shares is a random process and follows the same process as finding an acceptable hash for a network reward. The difference is that the pool accepts blocks with a lower difficulty. Skipping work could mean that the miner skips the work that would otherwise reward him with a higher share of the pool's reward as there is no know method to predict end result of the hash.

Pools have few different reward plans. Some have more risk for the miner, and some have less risk. For the pool, keeping servers available 24/7 is not free. For this reason pools take their own cut on blocks and on the transaction rewards. In bitcointalk forums developers and miners have had discussions whether the miners could increase their profits by jumping between two pools, which led to a few interesting papers on the subject of reward algorithms. According to Bitcoin Wiki [11], larger pools have all adopted pool hopping proof algorithms [37]. Another difference between pool and solo mining that the former offers is a reliable revenue stream and the latter the "gambling" revenue stream. "Reliable" pooled mining is somewhat more expensive because of the fees the operator takes. However, a miner with an average or lower hash rate hardware might want to receive a steadier revenue stream, even if the overhead is around 2-5 percent of the rewards.

3.2.1.2 Reward Algorithms

Marek Palatinus was the first one to create pooled mining, and naturally he created the first reward model. In a 2011 paper by "Raulo" [12], he raised questions concerning the fairness of giving rewards based on current work

[11] Bitcoin Wiki, 1.7.2013 `https://en.bitcoin.it/wiki/Comparison_of_mining_pools`

[12] Raulo,4.2.2011 `http://bitcoin.atspace.com/poolcheating.pdf`

share, where miner rewards are based on a single block share. The problem is that the time needed to find a rewarding block is not constant. In Palatinuses' pool, these rewarding blocks are sometimes found in one minute but have sometimes taken more than 17 hours.

Pool hopping means that the pool users change pools when they have generated a decent amount of shares to maximize rewards. For example, let us assume that a pool is unlucky, and has already taken more than three hours to find a block when the expected interval was 40 minutes. The miner then decides to transfer his computing resources to the other pool, preferably to one that has previously found a block. The share of the first volume that the user contributed will dilute, but also the reward per second will falls because it takes so long for the first pool to find a block. At some point, it became more profitable for the user to change to the another pool. It is not uncommon that a pool has to search for a block for hours, even when pools have 20-30 percent of the hash rate of the Bitcoin network, which would result in an expected interval of under an hour. However, some blocks will be found in under a minute, which usually cancels out the poor luck of those searches that took several hours for the people loyal to the pool. In contrast, people who change pool after an hour are likely to receive extra income from other pools because they already have shares in the first pool. When the average time for the pool to find the block has clearly passed, the miner gains more by hopping back to the another pool and by generating his share in the other pool until the first pool finds a block. It might well be that the second pool might find several blocks during this time, or it might not find any, but the user has gained shares in this pool and on average should acquire a higher total reward than what he would have obtained if he had remained loyal to the first pool.

Meni Rosenfeld explains how most of the used reward algorithms have solved pool hopping [37]. The reward algorithm of Palatinuses' pool changed in order to prevent users from acquiring benefits from pool hopping.

The most used reward algorithms appear to be PPS, score and PPLNS. PPS means pay per share and PPLNS means pay per last n shares. PPS solves the issue of pool hopping by rewarding miner for all submissions contributed to the pool. PPS pool's reward is formed from the predicted number of shares needed to find the block. This means an additional risk for the pool operator. This is usually reflected in a higher commission to the pool.

So called score based system basically consists of two types of "scoring" by which the reward is distributed. Pool assigns the first part from the shares that have been submitted to solve the current block and the second part comes from historical data, that ranks loyalty for the pool.

The historical data is basically a score that the miner obtains by staying

in the pool. If the miner leaves in the middle of a block search in the manner described earlier, miner looses some of his loyalty points, which will effect multiple blocks. The hoped effect of this reward algorithm is that instead of encouraging users to hop pools, it will encourage people to stay in the pool as long as possible.

The side effect of this reward algorithm is, thought, that the miners who use graphic cards for mining and gaming are punished because they usually cannot mine all the time. Instead, it rewards those who have dedicated mining equipment and a reliable internet connection.

PPLNS goes further than the score based system. Instead of combining the two score systems, it rewards the miner for the last N number of blocks. It has a similar effect to the score based system on the user. Depending on how long the user can mine, it might be more profitable to switch from PPLNS to the PPS pool, even though the pool commission is higher because dropping out of the pool also introduces a penalty. The historical score might also decrease the reward even more.

3.2.2 Why Mining is Necessary

Miners are an essential part of Bitcoin network because, without them, bitcoin would collapse since transactions would not be accepted. However, human nature is such that it is very unlikely that the Bitcoin network will ever suffer from a shortage of miners as long as people are willing to use bitcoins [3] because bitcoin network rewards miners with bitcoins for finding the approved block for the block chain. The Bitcoin network also balances the interest for mining with the algorithm that makes mining more computationally challenging as miners add more computational capacity is to the network.

Mining serves at least two purposes. The more obvious one is to check that transactions are valid. The other reason is to generate interest in bitcoins as a reward system to provide a steady increase of bitcoins for the network. The reward system is designed so that those who start mining at an early stage receive a higher reward because the reward is halved every 4 years. This means that people are encouraged to become part of the ecosystem as early as possible. It also means that the value of bitcoins increases over time if more people become interested in bitcoins. It could be argued that mining is actually a delivery system for new bitcoins, until year 2140. Then nearly 21 million bitcoins will have been generated and no more cannot introduced to the network.

It should be noted that from a technical perspective too, mining is necessary because it prevents double spending. It is impossible to spend the

same money twice with fiat currency, but with digital currency this is not a trivial matter, and basically, this was the fundamental innovation behind Bitcoin. In Bitcoin double spending has been solved by having only one miner to create valid block containing a group of transactions, and whoever checks the next group of transactions has to have a knowledge of the previous transactions. Part of mining is to check these transactions and to add them to a block. If a miner sends a block with a double spending transaction, the network will simply ignores that block and, the miner will not be rewarded.

Chapter 4

Communication in the Bitcoin Network

4.1 Bitcoin Protocol and Peer Discovery

Currently no central authority exists where the nodes can find the IP addresses of their fellow peers in the Bitcoin network. For this reason, each Bitcoin client has a ruleset to maintain consensus in the network. The nodes need to be able to spread blocks, transactions and other messages throughout the Bitcoin network. The Bitcoin protocol has three methods to discover users. Bitcoin nodes send so called "Addr" messages to the other Bitcoin users to request the addresses of the other Bitcoin users using DNS, IRC or previously known addresses. In the future, DNS seems to be the method that the Bitcoin network will eventually adopt instead of IRC [1].

The Bitcoin protocol supports the following messages: version, verack, getaddrs, addrs. inv, getdata,getblock, getheaders, tx, block, headers, ping, alert and submitorder.

The version message informs other peers on the Bitcoin version they are using. Verack is a version acknowledgement. Getaddr is a message to request peers to send their list of known nodes. The addrs message includes a lists of hosts known to node. It is response for the getaddrs message. The inv message informs other peers on which blocks peer currently has. Commonly, a node sends an inv messages when a node receives a new block. The Getdata requests the user to send either a single block or a transaction. Getblocks is similar to the inv message, but with a range flag, which means that node sends multiple items as a answer to this message. The Getheaders message

[1] Bitcoin wiki, 14.12.2013 "DNS is default mechanism as of v0.6.x" `https://en.bitcoin.it/wiki/Network`

is nodes requests message for the header information of blocks. As with the getblocks message, multiple headers can be requested. Tx is a transaction message containing transaction data. It is mostly used to answer an getdata request or a single transaction. The block message answers the getdata message, but instead of responding with a transaction, node sends a block that usually contains multiple transactions. Headers message is a answer to the getheaders' message and contains requested block headers of up to 2000 blocks. Ping is used to check the liveness of the peer, and alert messages are used to broadcast emergency messages to Bitcoin users [2]. Submitorder is used for sending bitcoins with IP-based addresses rather than with Bitcoin addresses.

Similarly to most peer-to peer-networks, NAT seems to be a problem also for Bitcoin. Regardless of the discovery method, the peers behind NAT might still not receive the incoming discovery messages. A NAT drops an incoming connection from another node, which is why the users behind NAT rarely find more than eight peers to connect with unless they have manually opened 8333 TCP port for Bitcoin. Eight is considered to be the minimum number of nodes the Bitcoin client should be connected to although a user behind NAT or the firewall rarely can connect the more nodes than this [9]. This is likely to be result of so many Internet service providers selling Internet connections with NAT on their end or giving pre-configured NAT modems to save public IP-addresses. End result is that new users cannot connect to user with NAT because NAT drops their connections, and similarly at start up other users with NAT drop users connections, leaving user with option to only connect users with out NAT.

4.1.1 IRC

The IRC was the preferred way to discover peers during writing of this thesis, although the Bitcoin Wiki, [3] states that this method is deprecated. When using the IRC method the Bitcoin client connects to the irc.lfnet.org server and joins one of the many Bitcoin IRC channels between bitcoin00-bitcoin99 on that server. When a user joins a channel, the client software parses the IP addresses of the peers currently connected to the channel from the user names. The Bitcoin client should use only those names starting with "u". It is followed by a 4 byte IP address, 2 byte port, and 4 byte Base58 encoded

[2]Jason Schaumleffel, Youtube, 23.5.2013 `https://www.youtube.com/watch?v=dEugZDI6O_Q&feature=youtu.be`

[3] Bitcoin Wiki, 23.12.2013 `https://en.bitcoin.it/wiki/Network`

checksum [4]. The reason for previous formatting is that the Bitcoin client can read the IP address from the IRC user names currently in the channel and request a node for the list of nodes known to it. For load balancing reason, unofficial Bitcoin client BitcoinJ randomly picks out a node from whom it requests the node list, and repeats this process until one of the nodes reply. In July, 2013 Bitcoin clients still did not seem to support IPv6, but no technical reason seems to exist to prevent IPv6 implementation.

4.1.2 DNS Lookup

The Objective behind DNS is to resolve the IP addresses from more easily remembered "name" address [11]. In the record section of the protocol, DNS operators can include multiple different addresses with multiple types. The way DNS lookup works is that Bitcoin client has multiple hardcoded DNS servers such as bitseed.xf2.org, dnsseed.bluematt.me as well as dnsseed.bitcoin.dashjr.org [5] [6] [7] which keep track of some of the Bitcoin nodes. When a user opens his wallet, it asks one of the DNS servers to give address of another user. This is repeated until received node answers to request to send his known node lists. Also, multiple DNS operators exists. This means that the DNS discovery is not so vulnerable to server downtime due to the net splits or similar problems that might occur in the IRC type of discovery.

The DNS lookup method allows multiple different types of DNS servers. Some servers, for example, can use the static address tables [8] for the most reliable hosts, but some support dynamic DNS for more ephemeral user records.

4.1.3 Hardcoded and Previous Addresses

Bitcoin clients such as BitcoinJ have multiple hardcoded addresses for reliable Bitcoin nodes. BitcoinJ calls these "SeedPeers" [9]. If the DNS lookup

[4] Google code, 7.7.2013 `https://code.google.com/p/bitcoinj/source/browse/core/src/main/java/com/google/bitcoin/discovery/IrcDiscovery.java`

[5] Pieter Wuille, Stack Exchange 2.5.2012 `http://bitcoin.stackexchange.com/questions/3541/how-secure-are-the-dns-servers-for-bitcoin`

[6] Bitcoin Wiki, 21.12.2013 `https://en.bitcoin.it/wiki/Satoshi_Client_Node_Discovery`

[7] Bitcoin Github 1.7.2014 `https://github.com/bitcoin/bitcoin/blob/master/src/chainparams.cpp`

[8] Static tables in this case means list of users that DNS server operator adds to configuration files

[9] Google code, 9.6.2013 https://code.google.com/p/bitcoinj/source/browse/core/src/main/java/com/google/bit

and IRC methods fail, the Bitcoin clients typically use these hardcoded addresses for discovery. Some clients gather previous known node addresses and use them before using these "hardcoded addresses"[10]. The client should randomly choose a client from either client list until one of the nodes answers by sending its list of known nodes.

4.1.4 Transmitting

In the Bitcoin network, transactions and blocks are transmitted through peers to each other. Each peer has to check the validity of the transaction prior to sending it to its peers [2]. The BitcoinJ code documentation notes that bitcoin miner has the final saying if the transaction is valid [11]. However, sending invalid transactions wastes bandwidth.

The Objective is that the node closest to the client broadcasts a transaction to its closest nodes until network includes the transaction to the block chain. The rest of the nodes ask their closest peers which transactions or blocks they already know and send the ones that the another node does not yet know. This should spread the transaction throughout whole network. Nodes always check the transaction prior to sending it to other nodes to filter out transactions or blocks that do not comply with the Bitcoin protocol rules.

4.2 Achieving Consensus

Interoperability Bitcoin test beds exist where developers can test their own client implementations without transferring any real bitcoins. Possibly because developers of the official Bitcoin want all implementations to comply to the same rules. Nodes with a faulty rule-set would be troublesome for Bitcoin because all nodes participate in filtering and distributing of transactions and some transactions considered valid by most nodes might not be distributed because of this. According to Kroll [18], new rules will create a new branch if a significant number of nodes accept the new rules. This would mean that the currency splits into Bitcoin A and Bitcoin B according to Kroll. Splitting of Bitcoin has already occurred once. This has been observed in an event when Bitcoin version 0.7 and 0.8 changed the rule set. This event created

[10]Bitcoin Wiki,1.1.2014 `https://en.bitcoin.it/wiki/Network`

[11]Google Code, 18.12.2013 `https://code.google.com/p/bitcoinj/source/browse/core/src/main/java/com/google/bitcoin/core/TransactionConfidence.java` Line 47 "miners have the final say in whether a transaction becomes valid or not"

its own branch for the Bitcoin clients with the version to 0.8, which was later ignored because the community decided to accept the 0.7 path to avoid splitting Bitcoin into two currencies. The problem was that the newer 0.8 version allowed a larger block size than 0.7 version. It caused older clients to branch into a different block chain than that of the 0.8 version users. Both clients thought their block chain was the correct one until the 0.8 branch was discarded as rules were changed to comply with 0.7 version rules.

Chapter 5

Energy Efficient Mining

This chapter discusses energy efficient mining and points out the common misunderstanding related to high computing performance translating into large profits. As explained later in this chapter Bitcoin mining equipment and electricity cost should also be considered.

Some well-known economists have pointed out that Bitcoin is a currency based on wasting resources. While this is not entirely true as profiting out of Bitcoin mining is actually requires user to create efficiency for bitcoin network. If miner fails to deliver efficiency he is actually loosing money no matter how fast mining device miner has. Some people argue bitcoin to actually "trade energy" [10].

Bitcoin mining as is essentially creating hashes of transactions and their container called block in a loop as fast as possible, which consumes a lot of processor cycles and therefore notable amounts of electricity. If someone could generate blocks and verify transactions more efficiently than others, he would receive a larger reward per watt. In time, the break-even efficiency bar rises and less efficient miners will begin to generate loss, while other more efficient devices will be able to generate even more profits.

When application specific integrated circuit (ASIC) miners came to market, networks computational capacity notably increased. Miners who got their ASIC miners before anyone else made thousands of dollars every day. Not only did these new ASIC devices possess a superior hash rate of 30 Ghash/s versus the GPU's 0.5 Ghash/s in 2013, but they also consumed less electricity compared to the GPU unit. The initial promise by Butter fly labs (BFL), which is one one the most known bitcoin miner manufacturer, for jalapeno ASIC miners was 1 watt per 1 Ghash, but eventually turned out to be between 2 and 3 watts per Ghash. Although this is not as much as with the GPU units, the Bitcoin currency still continues to use a significant amount of electricity. Bitcoin requires large amounts of computational per-

formance because the Bitcoin network is essentially a voting network, and it would not be in the best interest of Bitcoin if someone had a majority of the votes. This requires the network to possess enough computing resources to make it nearly impossible for one person or organization to gain over 50 percent of the resources.

This means that Bitcoin consumes electricity, but also tries to be as efficient as possible while doing so. For a fair comparison, Bitcoin's energy consumption should be compared to the consumption of Paypal or one of the giant banks, and not the number of households its power consumption is equivalent to. For example, one could ask if Paypal's consumption of electricity is more or less than the average electricity consumption of 31,000 households that has been calculated for Bitcoin, [1]?

5.1 Different Hardware

A lot of different hardware and operating systems can be used for mining bitcoins because clients exists for in Python, Java, and even some for Javascript. Especially Java and Javascript clients allow mining with a large set of devices. Unfortunately, the more common the hardware is, the more likely it is to be neither energy efficient nor economically viable for the miners. The reason for this is that the Bitcoin network adjusts the difficulty so that it takes approximately 10 minutes to find a new block. Thus, the more common the hardware setup, the more likely it is to be just wasting energy.

Some articles suggest that Bitcoin is creating currency by wasting resources, which in this context is electricity. While this is true to a degree, bitcoin mining rewards efficiency in order to save resources. Bitcoin network achieves this by ensuring that the necessary level of difficulty is recalculated every 2016 blocks, which occurs approximately every two weeks [4]. Thus, the network reassesses the profitable watt per hash every two weeks. The end result is that the inefficient miners become unprofitable sooner and are ultimately replaced by more efficient miners. However, some users just want to donate computing time and do not aim for profit. This is not unusual because multiple projects use Berkeley Open Infrastructure for Network Computing (BOINC) for different kinds of research that rely on users donating their computing time, which is somewhat similar concept with out the rewards bitcoin network hands out.

[1] Mark Gimein, Bloomberg12.4.2013 `http://www.bloomberg.com/news/2013-04-12/virtual-bitcoin-mining-is-a-real-world-environmental-disaster.html`

It seems mining software is available for most kinds of devices. The initial estimate was that multiple different performance categories exists for devices. X86 processors are the most obvious one, but because the user base of x86 is so large, it seems already uncompetitive and, therefore, unprofitable. Simply too many users possess access to this kind of hardware.

It is not easy to determine if ARM processors would be profitable either. Arm chips are very common, for example, in tablets and mobile phones. These common arm devices, however, possess a disadvantage when it comes to the initial investment since most of the common ARM devices such as phones are fairly expensive.

GPU is known to contain massive amounts of computing resources, especially when tasks are of a simple repetitive nature and do not affect each other's results. This type of work should scale well to the GPU. To cite bitcoin wiki: "Video processing is plenty of repetitive work, since it is constantly being told to do the same thing to large groups of pixels on the screen. In order to make this run efficiency, video processors are far heavier on the ability to do repetitive work, than the ability to rapidly switch tasks" [2]. In short, this is more or less the same reason why the GPU is so efficient at cracking hashes with the brute-force method. This has been explained in a two-part article in Linux Journal [35, 36].

It also seems that some manufacturer's design is superior to the others. December 2013, Bitcoin Wiki states that the AMD GPU units possess 2-3 times the performance of the Nvidia GPU units. On the other hand, the Tomshardware site states "Nvidia cards are typically slower by a factor of five to seven"[38], a figure also mentioned in an Extremetech's article [14]. This means that the GPU's can be divided into two classes of their own based on manufacturer. However, we did not consider this worth testing since AMD has been measured to have a much better product at the present for this purpose. Extremetech [14] explains that the reason for this is that Radeons possess a better instruction set and higher core count.

Additionally, dedicated mining devices exists. First to enter the market were the FPGA-based devices, which had a better efficiency compared to any GPU. Based on the Tomshardware article [38], we estimate that this was around one-fifth of the power consumption, while at the same time it is able to harvest more hashes than the GPU. However, since these dedicated Bitcoin miners cannot do anything else, such a devices have failed to acquire such a large market share. On the other hand, a gamer already possesses relatively high-end graphic card(s) to be used both on mining and gaming.

[2]Bitcoin Wiki 1.12.2012i `https://en.bitcoin.it/wiki/Why_a_GPU_mines_faster_than_a_CPU`

It could also be argued that gamers obtain their mining hardware free of any extra charge.

ASIC miner pre-orders were taken by Butterfly labs and some other companies, but very few were actually delivered before the summer of 2013. We managed to obtain one of these ASIC miners, which further expands the gap between the other devices and dedicated mining hardware.

Butterfly labs claimed that efficiency was going to be as high as 1 Ghash for one watt. In comparison, our high-end GPU consumes 150W for 0.5Ghash/s. As was pointed out earlier in this thesis, efficiency is the key to generating profit from Bitcoin mining, and, sooner or later, these dedicated miners may replace GPU-based devices similarly as GPUs did with CPU.

It will also be more difficult for someone to acquire resources that could hurt the Bitcoin network because botnets would have to have around 500 X86 PCs to compete with one ASIC miner, which costed around 150 dollars when per-ordered January 2013. BFL did not, meet this goal exactly with its first devices although it seems that botnets similar to those described in the "Case study of the Miner Botnet" [34] acquires drastically fewer bitcoins because hash rate rose so much. Higher efficiency of specialized devices means that, in time, non-dedicated devices become obsolete. The situation was reminiscent of a "gold rush" where the first people on the scene made large profits, and those who realized the opportunity too late had to compete with a huge number of people, which made profitability hard to achieve as same happened with ASIC miners. Those who were able to acquire one amongst the first were the ones making most profit.

One might wonder why a company would sell or rent dedicated Bitcoin miners. One is the storage of the devices and their cooling. Second and probably the most important reason is that no matter what occurs in the market bitcoin miners manufacturer will make a profit in any case. In a way similar to that of the gold rush days, when shovels and other equipment sold very well, equipment merchants did not have to worry about the miners' luck . BFL and others who are designing mining devices are selling devices to customers in a market where the second cheapest miner costs 1200 dollars. At the same, time people willing to buy miners are taking the risk while BFL has their money secured.

5.2 Data Analysis of the Miners Hash Rates

In this section, we analyses how many users are donating their computing time to Bitcoin without obtaining any money from mining. Unfortunately, no open statistics is readily available to estimate what kind of devices

users have. Andrew Geyl, however, was kind enough to supply data from few mining pools, which allows us to estimate the user-specific hash rate. Data contained account specific hash rates of pool users. It included pools such as Bitclockers (27.1.2013), BTCGuild (27.1.2013), Eligius (27.1.2013), FiftyBTC(27.1.2013), HHTT (27.1.2013) Itzod (27.1.2013), p2Pool (27.1.2013), Polmine(27.1.2013), Bitminter (21.4.2013), Slush (27.1.2013) and Ozcoin (5.5.2013).

5.2.1 Profitability

We decided to estimate how many users are generating less than 100 Mhash/s from Geyl's data. 100 Mhash/s was chosen because these devices are either low efficiency GPU or CPU, and we assume that none of these users are hopping between pools as most pools punish users for doing it.

From Andrew Geyl's dataset we gathered that 25 500 out of the 69 205 miners are generating less than 100 Mhash/s, which is a bit over 36.8%. Further analysis of this dataset is difficult because the data is account specific rather than device specific. To be more specific one account, can be associated with multiple mining devices. Therefore, it is difficult to distinguish if someone has hundreds of ARM computers or one highly efficient miner. However, since pools punish miners for jumping between pools, we assume that the number of users spreading work to multiple pools is very small. It is most likely done as a backup measure if a user cannot connect to his primary pool.

In the next figure, Andrew Geyl's dataset has been illustrated to show each users' hash rate. Large number of users are generating 100 Mhash/s or less as illustrated in Figure 5.1.

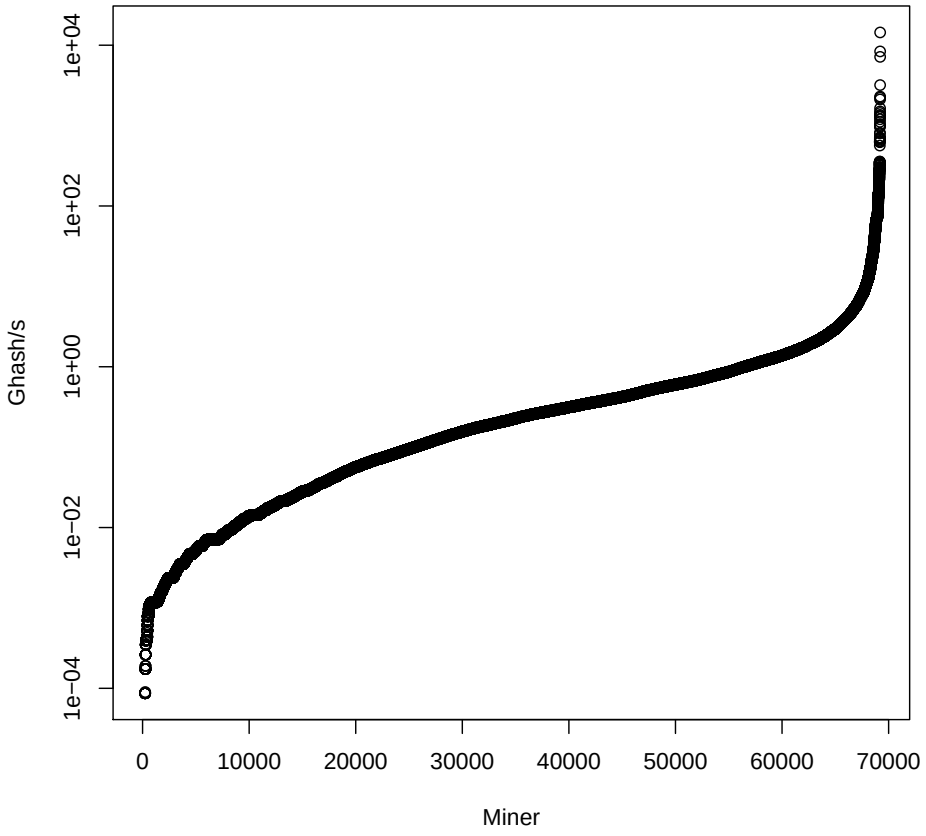

Figure 5.1: Miner hashrates below 15 Ghash/s

5.2.2 Assessing Profit and Loss

At a more detailed level, multiple different online calculators exists, which allow an user to estimate if they are making profit. Some try to estimate the increase in difficulty, which affects long-term mining profits. The formula shown below calculates the income of Bitcoin mining.

$$\frac{OHashrate}{NHashrate} \times \frac{[RoundReward + TXRewards]}{600s} = \frac{Income(BTC)}{s} \quad (5.1)$$

Here OHashrate is the user's own hash rate, Nhashrate is the entire Bitcoin's network hash rate. Most calculators calculate Nhashrate from "the network difficulty", which changes every two weeks. The objective here is to calculate the user's portion of the hash calculation that the user adds to the network,

which is basically the degree of likelihood of the user receiving the reward. The network reward illustrated as RoundReward is the lottery reward that the network rewards one miner or pool on average every 10 minutes i.e 600 seconds. In addition to this, the winning miner also receives transaction rewards marked as TXRewards in figure. The total transaction reward is dependent on the number of transactions, and to what extent the users making the transactions paid the transaction reward. Users are free to offer any amount, but miners prioritize transactions based on the reward.

To assess the actual profit, it is necessary take into account the electricity and hardware costs as shown below.

$$\frac{Profit}{s} = \frac{Income}{s} - \frac{ecost}{s} - \frac{Hcost}{s} \tag{5.2}$$

In reality it is very difficult to determine profitability. Not only does it involve the estimated value for bitcoin, but also the electricity price, transaction rewards, equipment, and maintenance costs too. Electricity cost per second is shown in equation as ecost/s. The more difficult one to calculate is device cost per second shown as Hcosts/s, unless device has been rented. Otherwise, estimating how long device can profitably mine is difficult. In many cases, it is also difficult to determine the hardware cost because some devices have other uses than just mining. Mining might be done only when the equipment is idle, and in that case the actual equipment costs would be higher than "wear and tear" costs that could be applied as cost of mining.

Not even electricity costs are a trivial matter to calculate. In some countries such as Finland, heating is required for most of the year. Bitcoin miners could, for example, use the heat generated by their mining devices for heating. In contrast, in some countries, cooling is required, even when nobody is mining bitcoins. It could be argued that bitcoin miners could be used as heaters in cooler climate areas and thus at least "waste" less electricity than they otherwise would.

Mining can be considered as analogous to the situation of having lottery tickets weighted with the hardware's performance in order to generate block hashes. The difficulty is changed every 2 weeks. Therefore, the Bitcoin network's hash rate should be considered an average of this value.

In the paper on mining reward systems by Rosenfeld [37], a different formula is introduced that takes into account the variance when miners mine in pools . The conclusion is that the larger the pool and the smaller the miner, the more profitable it is for miner to mine in pools.

Chapter 6

Performance Measurements and Analysis

6.1 Testing methods

In this thesis we tried to cover various types of Bitcoin mining devices. Unfortunately some devices, such as the FPGA dedicated mining devices, were too expensive to acquire. However, some low energy consumption devices, for example single and multi-core ARMs, have been included in our tests. Our devices include X86 processors, GPUs, and we also purchased a less common dedicated ASIC miner from ButterFly labs that is capable of 30Ghash/s, is called "Little Single". The devices tested were as follows:

Class	Name	Mining unit(s)	OS	Miner	Notes
CPU	Pandaboard	ARM (2-cores)	Ubuntu 12.10	Cpuminer 2.3	No mouse or keyboard
CPU	Raspberry PI	ARM (1-core)	Wheezy 16.12.2012	Cpuminer 2.3	No mouse or keyboard
CPU	Intel i7 920	X86 (4-cores)	Ubuntu 12.10	Cpuminer 2.3	
CPU	Intel Atom D510	X86(2-cores)	Linux Mint 14	Cpuminer 2.3	
CPU	E-350 Linux CPU	X86 (2-cores)	XUbuntu 13.04	Poclbm 20120920	
GPU	E-350 Linux GPU+CPU	X86+GPU	XUbuntu 13.04	Poclbm 20120920	
GPU	E-350 Linux GPU	GPU	XUbuntu 13.04	Poclbml 20120920	
GPU	E-350 win GPU	GPU	Windows 7	Poclbm 20120920l	
GPU	E-350 win HD 7950 GPU	HD 7950 DCII TOP	Windows 7	Poclbm20120920	
GPU	E-350 win HD 7950 GPU + CPU	HD 7950 DCII TOP with CPU	Windows 7	Poclbm 20120920	
GPU	Desktop qx9650 HD7950 GPU	HD 7950 DCII TOP	Windows 7	Poclbm 20120920	
GPU	N53JQ laptop geforce 425M GPU	Geforce 425M	Windows 7	Poclbm 20120920	
GPU	Mac mini GPU	geforce 325M	OSX	Bitminter 1.4.3	
GPU	Mac mini GPU	geforce 325M with CPU	OSX	Bitminter 1.4.3	
ASIC	ASIC Litle single	ASIC	Windows 7	Bfgminer 3.1.1	Dedicated miner

We tested multiple types of devices, such as X86 based laptops and desktops, and ARM-based devices. Also a GPU card, Mac mini with and without a integrated GPU were tested in addition to an AMD APU, which has a GPU integrated to a CPU. The previous table explains the various classes of devices. Devices are divided into three classes on the first column: CPU, GPU and ASIC. In the next column describes the names also shown in other graphs in this chapter. All devices use their default clock speeds. This is followed by the operating system, then name of the mining software. Finally, the last column, shows some additional notes. Unfortunately, no single mining client exists that could be used for all the devices. Based on our tests, we assume that the difference between different mining clients is small. Different mining clients offer different features, which may be more of a concern to the end user rather to than to raw performance. For example, Pocbm offers scheduling control, allowing gamers to determine the value of the desired frame rate per second for their game. It can perform a similar scheduling for a 2D environment by, for example, allowing movies to play at a constant 24 frames per second rate.

BFGminer offers an “intensity” setting that is different from the Poclbm frame rate limit. It seems to be similar to ”nice” in a Linux environment, which is not as precise as the Poclbm's minimum frame limit, but seems to be able to get higher hash rate out the devices, although, practically making machine unusable for other tasks while reaching best hash rate performance. Therefore, it is preferable to use BFGminer on dedicated miners.

GUIminer, which is a client for Windows, is only a user interface for Poclbm. However, it works both in Linux and Windows operating systems. Thus GUIminer is useful for those with less experience with command line.

Another user-friendly client is called Bitminter. It is a cross-platform Java-based client. However, Bitminter can only be used in one specific pool, and, therefore, ties the user to that pool. Also, it seems to be the least efficient mining client we tested.

In most tests, an electricity meter called Plugwise was used. It was chosen because the price-quality ratio is good and the error bounds are well understood as shown in the comparison of end user electric power meters for accuracy in a paper by Lassi Liikkanen [21]. Also second meter bought from Lidl was shown in the test.

The dedicated ASIC miner arrived later than we expected and Plugwise was not available for the measurements anymore during this time. For this reason, we used Lidl's consumption meter, which had a slightly higher variance according to Liikkanen's paper. Unfortunately, the Plugwise meter does not show decimal values, which means that lower power devices are not as accurate.

The tests were also conducted with different mining devices, and, the same miner could not be used in every operating system or processing unit. For example, not all processors support OpenCL nor did their graphic chips have drivers available with OpenCL support. Mining clients for the Mac platform were not supported, which is why a Java-based client was used on Mac.

We gather average value of power consumption with plugwise meter by mining multiple hours. We monitored hash rate for a half an hour to estimate the lowest and maximum power draw, which was usually easy because the hash rate did not vary much. The only exception was with the E-350. While the CPU of the E-350 processor was mining concurrently with HD 7950, the system appeared to suffer from some kind of scheduling problem. In this case, the CPU was under a 100 percent load, while the GPU occasionally did not seem to have any work to do at all.

We measured power consumption of most devices from the full system consumption. The one exception was when we were reading the relation to the ASIC miner device's power consumption. While all the other devices included the whole system, in the case of ASIC which is accessory device we felt that, because of the broad range of devices it can be connected, it would make little sense for us to find least power consuming device to test its consumption with the ASIC. Therefore, we decided to calculate only the electricity consumed by the miner as it has its own power supply. Even Raspberry Pi should be sufficient, which would only add between 2.5W and 3.5W to power consumption levels.

6.2 Results

This section describes results of measurements. We present two different kinds of diagram sets. Power draw and efficiency diagrams. Former shows the power consumption of the devices and it is followed by the diagram showing the power draw of a discrete GPU, which is the "HD 7950 TOP" from ASUS. The objective was to illustrate the amount of electricity the card uses. The latter part is about the efficiency charts, which exclude the ASIC miner device. The next diagram then compares the highest efficiency systems we tested with the ASIC miner. The last figure compares the performance of the FPGA device with the ASIC and GPU mining devices.

Figure 6.1 shows that the systems with discrete GPUs consume electricity the most; The top two systems use the HD7950 graphics cards, but the cheaper E-350 system consumes less electricity. On average, the third most electricity hungry system was the i7 920 system, which is a one generation

newer than the qx9650 system.

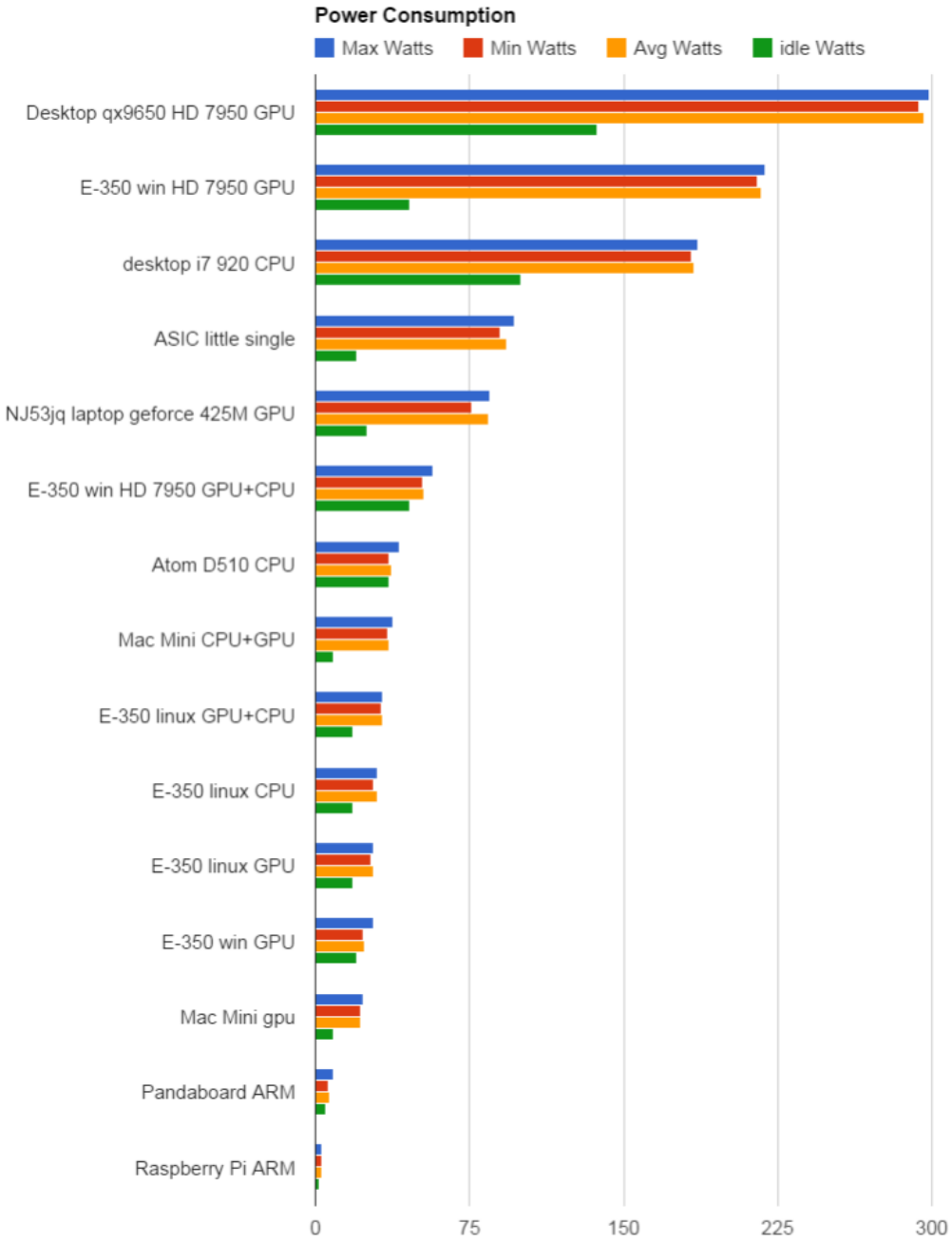

Figure 6.1: Power consumption of the tested devices

The fourth device is an ASIC miner little single, but unlike the others it does not include the power consumption of system it is attached to. Raspberry Pi B-model would increase consumption additional 3.5W, however, it

would not change its fourth position. It is followed by the Asus i7 N53JQ laptop. The N53JQ has the same re-branded integrated GPU as the Mac mini, but in this case, Mac's GPU does not offer same performance. The hash rates of these two are 14.2Mhash/s for the N53JQ and 6.5 Mhash/s for the Mac mini without involving the CPU in bitcoin mining and 6.6 with the CPU and GPU. When the E-350 concurrently uses both the 7950 discrete graphic card and its own CPU the E-350 ranks between the N53JQ and the Mac mini. It should be noted that the mining jobs could not be transferred to the GPU while the CPU load on E-350 was high. Next is the Atom D510, which is the direct competitor of the E-350 from Intel. Unfortunately, Intel decided not to include the PCI-express with the board, which means the D510 can only mine with the CPU. In CPU mining, the D510 has clear advantage over the E-350, with the E-350 generating 0.1 Mhash/s and the D510 mining at a speed of 0.76 Mhash/s. To put these in perspective, the Radeon HD 7950 in either qx9650 desktop or E-350 was able to generate around 450 Mhash/s. The ASIC unit speed is approximately 30 000 Mhash/s. We had a few different setups for E-350. It should be noted that with Linux, the E-350 actually draws more electricity than with Windows 7. It also seems that a very small gap exists between the CPU only and integrated GPU mining in terms of electricity consumption. However, the hash generation speeds differs noticeably. The E-350 achieves 0.1 Mhash/s with its CPU, but in the E-350 GPU's case, the hash rate is between 10 and 8 Mhash/s, where the higher value is achieved with Linux and the lower value with Windows.

Mac mini with only GPU mining is the last non-ARM device in the set. It had only a 0.1 Mhash difference between CPU and CPU+GPU mining, though CPU+GPU consumed more electricity.

Pandaboard had two cores and each of them was faster than one on Raspberry Pi. It could be argued that it is a decent System on Chip (SOC) in terms of performance when compared to the X86 alternatives, the E-350 or D510. Unfortunately, mining with these ARM-based devices is slow. Neither of the ARM chips is a viable option for mining anymore because none has a PCI-express to support a discrete GPU to be added for the ARM SOC. In brief, the ARM processor does not have the efficiency level of the GPU units nor ASIC.

The data of the 7950 TOP card in Figure 6.2 is based on cards own diagnostics for power consumption. It indicates that the graphic card's GPU consumes around 125W. Also, it can also be observed that the electricity draw fluctuates noticeably. The diagram was drawn from the values that GPU-Z software reported. It consists only of the power draw of the GPU and excludes the power draw of the other components, such as the graphic card memory. The graph only covers a 20 minute period, and it illustrates

a few things. First, a gap exists around 120W that the GPU rarely exceeds. Second, the consumption for the GPU is not steady. In many situations, part of the GPU is waiting for jobs to be executed. This means that performance could be improved by optimising the OpenCL drivers of the Radeon card or the OpenCL miner implementation. GPU-Z cannot time stamp accurately enough to distinguish how long each of these energy consumption drop last. Therefore, it can be only said that energy consumption changes multiple times in a second. In an optimal situation power consumption would be steady.

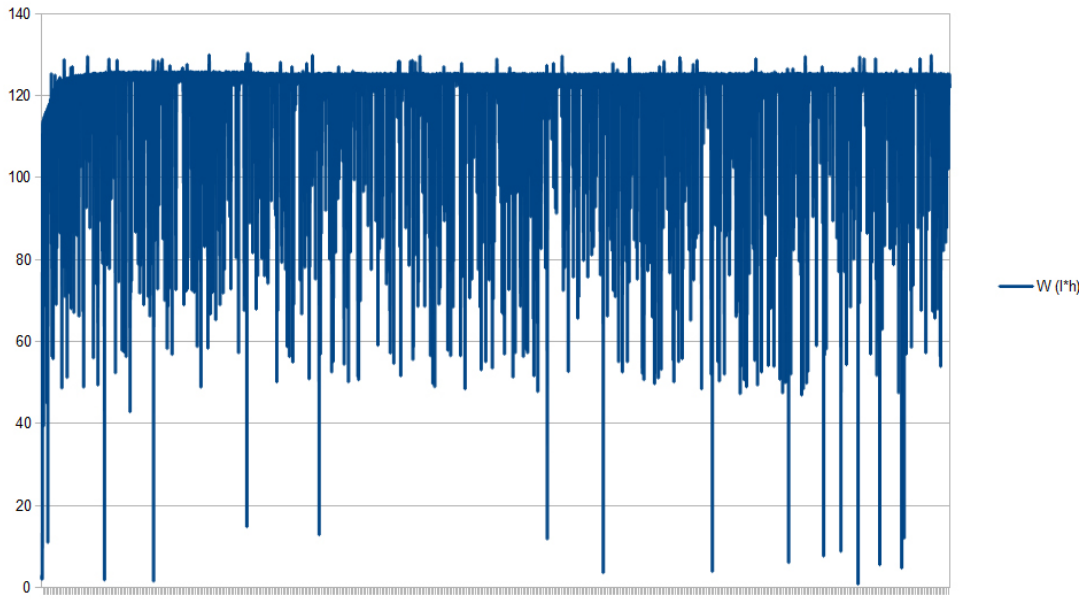

Figure 6.2: Power consumption of tested devices

During mining Figure 6.3 shows the average Mhash/s per Joule, in addition to Mhash per Joule from delta between mining and idle state consumption. The ASIC figures are broken down into two separate figures, 6.3 and 6.4, to clearly show the differences between ASIC and non-ASIC miners. The ASIC miner has such an efficiency advantage that any other device would seem to be equally inefficient in comparison. Namely, the ASIC miner has an efficiency of 320 Mhash/J, and None of the other devices tested were able to break 3 Mhash/J. The closest was the low-powered AMD E-350 with its discrete HD 7950 graphic card with 2,07 Mhash/Joule and with idle consumption reduced 2,63Mhash/Joule.

Mac mini seems to be more efficient than the N53JQ laptop, even though they have the same GPU.

Using a CPU and GPU concurrently seems to reduce efficiency. Most

obvious reason for this is that CPU has lower efficiency and thus drags overall efficiency down. It can further be seen from the less efficient devices at the top of the figure 6.3 that X86 CPU is inefficient. D510 also seems to have power consumption of 36W in idle and 41 during mining, which means that mining does not cost much when the machine is already on.

D510 is not a desirable alternative to E-350 for mining. As seen from its efficiency figure, E-350 has a large advantage in efficiency over the D510 CPU. In figure 6.3, ARM solutions rank below X86 CPUs. Raspberry does not have a similar hash rate to Pandaboard. Pandaboard uses more electricity, but has two cores and, thus, it is more efficient than Raspberry.

Next, we discuss the measurements on the GPU units with different setups. It should be noted that even though the power consumption of Linux Ubuntu was higher than with Windows, it also had a higher hash rate. The most efficient systems are the somewhat traditional desktop PC and E-350, both with a discrete graphics card, the Asus Radeon 7950 TOP. The PCI-express in the E-350 board had enough bandwidth to feed mining jobs and, therefore, performed well compared to the old high-end desktop PC. The old high-end system performed only 5Mhash/s faster than E-350. E-350 performed 450 Mhash/s, while qx9650 performed 455 Mhash/s. Neither the E-350 with HD 7950 nor the qx9650 system with 7950 had the efficiency of the ASIC miner.

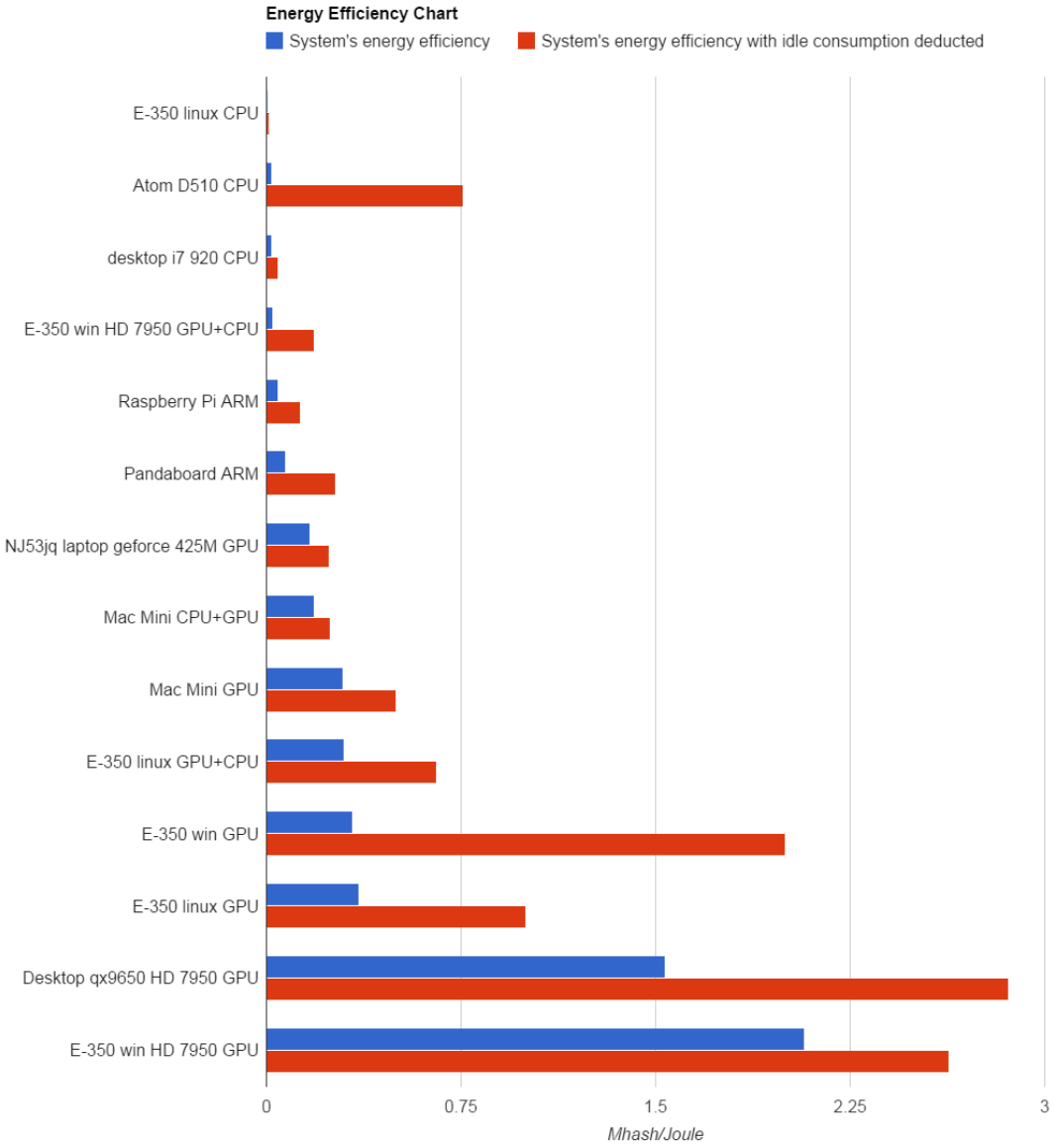

Figure 6.3: Efficiency chart Part 1

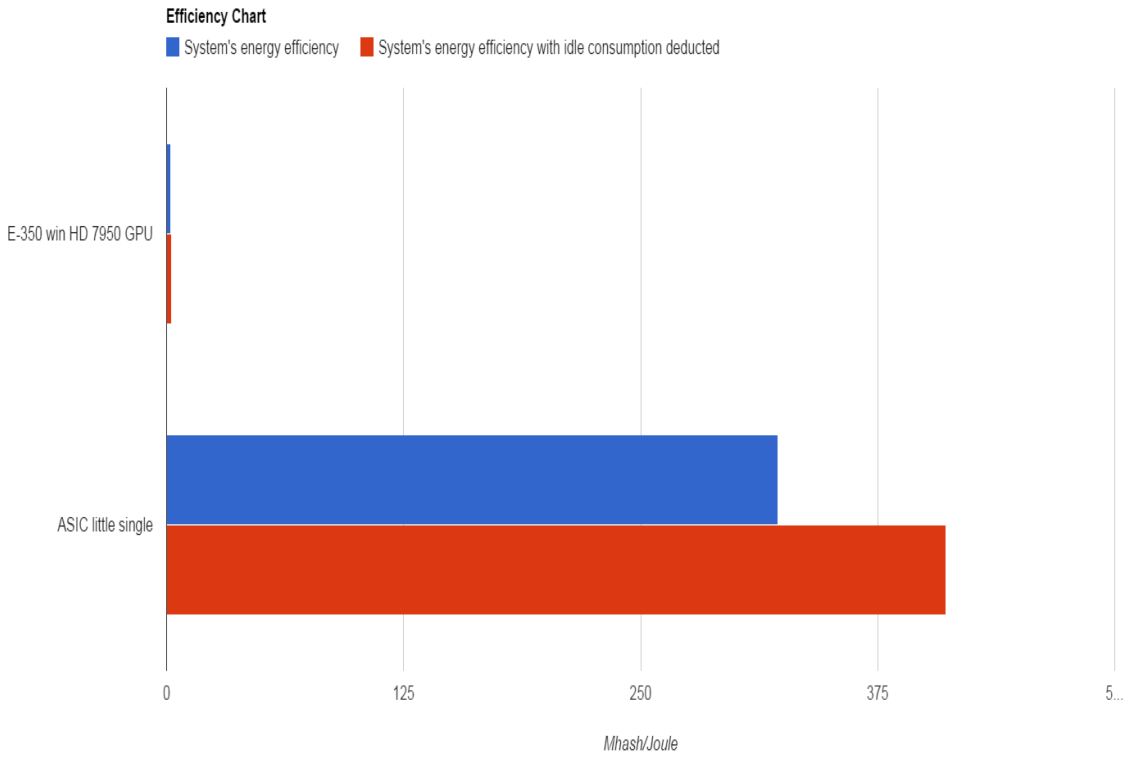

Figure 6.4: Energy efficiency chart Part 2

Since our test did not include an FPGA unit, we reference measurements from the Tomshardware guide [38]. Figure 6.5 shows that while FPGA unit is nearly five times more efficient than GPU powered device, neither the GPU device nor the FPGA is near the efficiency level of an ASIC.

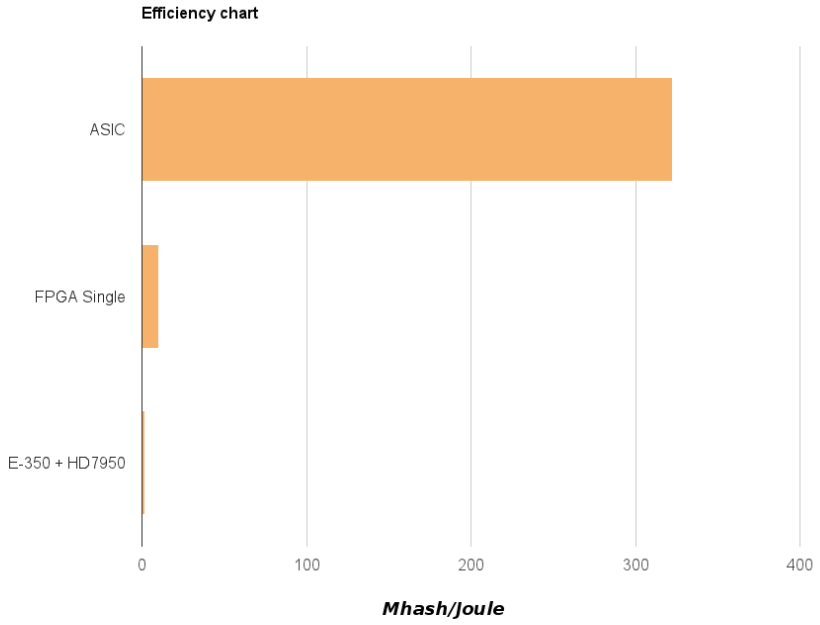

Figure 6.5: FPGA Comparison data for the FPGA unit from TomsHardware review [38]

6.3 Analysis

In this section, we categorize the devices into different classes, and draw further conclusions from the test results

6.3.1 Findings

It seems that Windows 7 scheduler did not work very well with the Poclbm bitcoin miner when we tested mining using E-350 CPU and the discrete GPU unit at the same time. At least, with AMD 13.4 drivers and Windows 7, we experienced some kind of scheduling problems since the CPU did not feed jobs to the GPU fast enough. This meant that GPU was mostly idle.

From these findings it can be concluded that it is not wise to use the CPU for mining to increase profitability because it might reduce the overall amount of computing capability. Also, some other idle operations come as a surprise, for instance, the Mac mini uses less electricity than the Asus laptop.

In contrast, Linux seems to be somewhat more efficient in an idle state than Windows on E-350.

In general, the highest consumption occurred on the GPU, followed by the high-end CPU bitcoin miner, then low-end low-power x86 CPUs and, lastly, the ARM CPUs. It should be noted that even the high-end qx9650 CPU system and the cheapest high-end graphic card from the AMD together with various hard drives have a power consumption of 300Watts.

Related to the power consumption figure, a few points need to be noted. The efficiency difference between top two systems is 2.07Mhash/s per Joule and 1.54Mhash/s per Joule, while both are using same Radeon 7950 GPU. However, the power draw of the qx9650 system is nearly 80W more. In other words, it is important to have a system with fast graphic card rather than fast CPU to mine more bitcoins in energy-efficient manner. Figure 6.3 shows that it is not important to have a high-end CPU since E-350 was a slower than Pandaboard in mining.

Pandaboard achieves 0.53 Mhash/s, while the E-350 performs at 0.1 Mhash/s. This means GPU mining should not only be on the hashing efficiency of the GPU, but also energy efficiency of the underlying system. At the beginning of 2013, the E-350 was top hardware for GPU mining. It was a low-end system, but also had a PCI-express connection sufficient for a discrete GPU.

It is also noteworthy to mention that ARM based Raspberry and CPU-only E-350 were able to generate blocks only when pool was unlucky. During our mining sessions in Palatinuses' pool, we experienced periods of over 17 hour when no blocks were found by the pool. Most of the time, however, these devices did not manage to find any shares prior to the pool finding a block, thus, meaning device did not get any share of the reward. In this case, it would have been more profitable to mine solo than in pool. In other words, mining with energy efficient hardware does not make sense even in a large pool when the mining hardware has very low computing power.

	Max watts	Min watts	Avg Watts	Idle Watts	Mhash	System's energy efficiency (Mhash/J)	System's energy efficiency with idle consumption deducted (Mhash/J)
Raspberry Pi ARM	3.00	3.00	3.00	2.00	0.13	0.04	0.13
Pandaboard ARM	9.00	6.00	7.00	5.00	0.53	0.08	0.27
Mac Mini gpu	23.00	22.00	22.00	9.00	6.50	0.30	0.50
E-350 win GPU	28.00	23.00	24.00	20.00	8.00	0.33	2.00
E-350 linux GPU	28.00	27.00	28.00	18.00	10.00	0.36	1.00
E-350 linux CPU	30.00	28.00	30.00	18.00	0.10	0.00	0.01
E-350 linux GPU+CPU	33.00	32.00	33.00	18.00	9.83	0.30	0.66
Mac Mini CPU+GPU	38.00	35.00	36.00	9.00	6.60	0.18	0.24
Atom D510 CPU	41.00	36.00	37.00	36.00	0.76	0.02	0.76
E-350 win HD 7950 GPU+CPU	57.00	52.00	53.00	46.00	1.30	0.02	0.19
NJ53jq laptop geforce 425M GPU	85.00	76.00	84.00	25.00	14.20	0.17	0.24
ASIC little single	97.00	90.00	93.00	20.00	30,000.00	322.58	410.96
desktop i7 920 CPU	186.00	183.00	184.00	100.00	3.80	0.02	0.05
E-350 win HD 7950 GPU	219.00	215.00	217.00	46.00	450.00	2.07	2.63
Desktop qx9650 HD 7950 GPU	299.00	294.00	296.00	137.00	455.00	1.54	2.86

Figure 6.6: Hash rates and energy consumption

The profitability changes constantly because of the nature of Bitcoin. Not only will the profitability of bitcoins differ, but the same also applies also the costs of electricity and devices . To estimate the profitability, operating costs have to be known.From the hash rate data shown in Figure 6.6, we can calculate the operating costs if the total hash rate of the network is known. For illustrative reasons, we have chosen the total hash rate of the network from July 2013. This provides an estimation for operating costs of each device as shown in Figure 6.7.

	Watts per block	Watts per bitcoin	Consumption cost to generate block of bitcoins (€)	Consumption cost to generate one bitcoin (€)
ASIC Miner	95,903.67	3,836.15	14.39	0.58
E-350 win HD 7950 GPU	14,918,348.15	596,733.93	2,237.75	89.51
Desktop qx9650 HD 7950 GPU	20,125,831.50	805,033.26	3,018.87	120.75
E-350 linux GPU	86,622,666.67	3,464,906.67	12,993.40	519.74
E-350 win GPU	92,810,000.00	3,712,400.00	13,921.50	556.86
E-350 linux GPU+CPU	103,909,414.76	4,156,376.59	15,586.41	623.46
Mac Mini GPU	104,708,717.95	4,188,348.72	15,706.31	628.25
Mac Mini CPU+GPU	168,745,454.55	6,749,818.18	25,311.82	1,012.47
NJ53jq laptop geforce 425M GPU	183,005,633.80	7,320,225.35	27,450.85	1,098.03
Pandaboard ARM	408,597,484.28	16,343,899.37	61,289.62	2,451.58
Raspberry Pi ARM	713,923,076.92	28,556,923.08	107,088.46	4,283.54
E-350 win HD 7950 GPU+CPU	1,261,264,102.56	50,450,564.10	189,189.62	7,567.58
desktop i7 920 CPU	1,497,985,964.91	59,919,438.60	224,697.89	8,987.92
Atom d510 CPU	1,506,127,192.98	60,245,087.72	225,919.08	9,036.76
E-350 linux CPU	9,281,000,000.00	371,240,000.00	1,392,150.00	55,686.00

Figure 6.7: Cost table

The cost of electricity is set at 0.15 euros, which includes both transfer costs and the actual electricity cost. In figure 6.7, it is also assumed that the hash rate of the network is 185620 Ghash/s. As shown in the figure, the first device to be profitable, when the bitcoin's value was around 200 euros, is the system with the discrete graphic card. When using a more efficient system, consumption cost was reduced by 30 euros per bitcoin. The ASIC miner from BFL, which appeared on the market at the end of summer 2013, is very profitable because it reduces the energy consumption costs to a nearly half a euro per bitcoin. We used the following formula to calculate the energy usage in the spreadsheet:

$$\frac{NHashrate}{OHashrate \times 6} \times \text{“Avg consumption”} \tag{6.1}$$

The first fraction is the network hash rate divided by devices own hash rate. First fraction in formula 6.1 gives us average number of blocks that need to be solved prior to finding an acceptable block. This value is divided by six because blocks are generated on average six times in an hour, which gives us the number of hours required to generate these blocks. Then the resulting value is multiplied by the average consumption of the device to estimate the total average energy consumption prior to finding a block. Result of the formula 6.1 can be found in the first column of figure 6.7 .

For the second column, this value is divided by 1000 to acquire for conversion into kW/h, which is normally the unit electricity companies charge. Then, we multiply that with the total electricity cost that was set to 0.15 euros per kW in the figure. To acquire Watts required to find one bitcoin, the Watts value in first column is divided by amount of bitcoin granted in a block, which at the time was 25. Similarly blocks electricity mining costs value is divided by 25 to get amount of euros required to mine one bitcoin. The calculation does not take into account the transaction rewards, which vary too much to form an estimation. However, since reward from blocks decreases by half every 4 years. Eventually, transaction reward will be the only reward the miners receive.

6.3.2 Categories

It could be argued that there are a few different classes of mining devices. However, due of the nature of IT, every device cannot be fitted into these categories as new products are constantly becoming available.

The first one is the CPU category, which consists of ARM and X86 based processors. ARM processors use very little electricity, but their capability to

calculate double hashes is also low. As illustrated in this chapter, ARM systems are still more efficient than the tested X86 processor. We estimate the performance of this category to be somewhere between 0 and 100 Mhash/s. The efficiency of this category is the worst of those compared and, therefore, is very unlikely to generate any considerable profit.

The second category is defined as the higher-end AMD GPU category. This consist of graphic processing units and, for example, AMD APU is not included in this category because it is basically the AMD's view of a CPU, which has a GPU integrated in the processor. The APU's performance should be somewhere between a high-efficiency CPU and a medium-to-low efficiency GPU. This category does not include Nvidia GPU units either because, according to Bitcoin Wiki's hardware comparison (21.7.2013), the high-end 680 GPU generates 110 to 127 Mhash/s in comparison with the AMD's high-end 7950 GPU that generates 450 to 550 Mhash/s [1].

The third category is the first wave of specialized Bitcoin units. In comparison, Bitcoin Wiki does not mention any graphic card with an efficiency of 4 Mhash/Joule or more. This first wave of dedicated miners can be described as specialized Bitcoin units with a minimum efficiency of 10.4Mhash/Joule, and the highest efficiency of 23.25Mhash/Joule [2]. Therefore, the efficiency is more than 10 times the efficiency of the GPU unit in our tests. Unfortunately, the hash rates of these devices overlap with the previous higher-end AMD GPU category because the devices in this class have a hash rate between 100 and 25 200 Mhash/s. The best devices can generate 25 200 Mhash/s but cost 15 295 euros. Thus, we limit this category to between 100 and 860 to more easily distinguish it from the next ASIC category.

The fourth and final category is the ASIC category. It consists of a second wave of specialized Bitcoin units. Most of these devices achieve a higher hashrate than 4500 Mhash/s. The most expensive device available for pre-order from BFL was capable of 1 500 000 Mhash/s at 21.7.2013.

To estimate profitability, the point of efficiency has to be determined. This is the point prior to which Bitcoin mining ceases to be profitable. Unfortunately, as the FPGA and GPU units hash rates overlap in our categories and also have a huge efficiency difference, it is difficult to distinguish whether some randomly picked miner is using a 300 Mhash/s graphic card or higher efficiency FPGA device.

[1] Bitcoin Wiki, 17.12.2013 `https://en.bitcoin.it/wiki/Mining_hardware_comparison`

[2] Bitcoin Wiki 10.8.2013. `https://en.bitcoin.it/wiki/Mining_hardware_comparison`

6.3.3 Mining Prospects

It seems that GPU mining follows the fate of CPU mining according to our results. While ASIC hardware is only capable of generating bitcoins, its efficiency seems to be over 100 times greater than with GPU. The entry price of ASIC pre-order, at least in 2012, was not high. A entry unit capable of 5 Ghash/s costs 150 dollars. It has the same efficiency rating as our ASIC "Little Single".

Techspot news [3], and also Symantec's blog, [4] mentions that Bitcoin mining with CPU generates less than half a dollar a year with their test machine. This means that the electricity cost is higher than the immediate profit from mining of bitcoins, and thus it would be cheaper to just buy bitcoins from the Bitcoin exchanges.

It is important to have mining equipment with high hash rate, but efficiency is the key to profit from Bitcoin mining. As ASIC has 100 times better efficiency than GPU, it is difficult to imagine GPU mining being profitable. CPU mining is already unprofitable and the ARM chips are not even able to submit results to the pool before someone had already found the block. The following figures 6.8 and 6.9 illustrate the costs of electricity in euros to generate one bitcoin whether it is possible or not during one month. The electricity price is again set to 0.15e/kW and the Bitcoin network's hash rate for each month has been obtained from the block chains.info [5]. It might not be obvious, but the costs of mining follow the Bitcoin network's hash rate as later illustrated in Figure 6.10. Figure 6.8 shows all the miners on a logarithmic scale to show the difference between the devices. This figure does not show exactly the amounts, therefore separate figure for Pandaboard was drawn to illustrate the similarity to Bitcoin network's hash rate graph. Figure 6.9 illustrates the electricity costs of the most efficient CPU mining system tested, which was Pandaboard.

[3] Shawn Knight, Techspot 1.10.13 `http://www.techspot.com/news/54194-symantec-grapples-with-one-of-the-largest-botnets-in-history.html`

[4] Symantec, 1.10.13 `http://www.symantec.com/connect/blogs/grappling-zeroaccess-botnet`

[5] BlockChain 30.11.2013 `https://blockchain.info/charts/hash-rate`

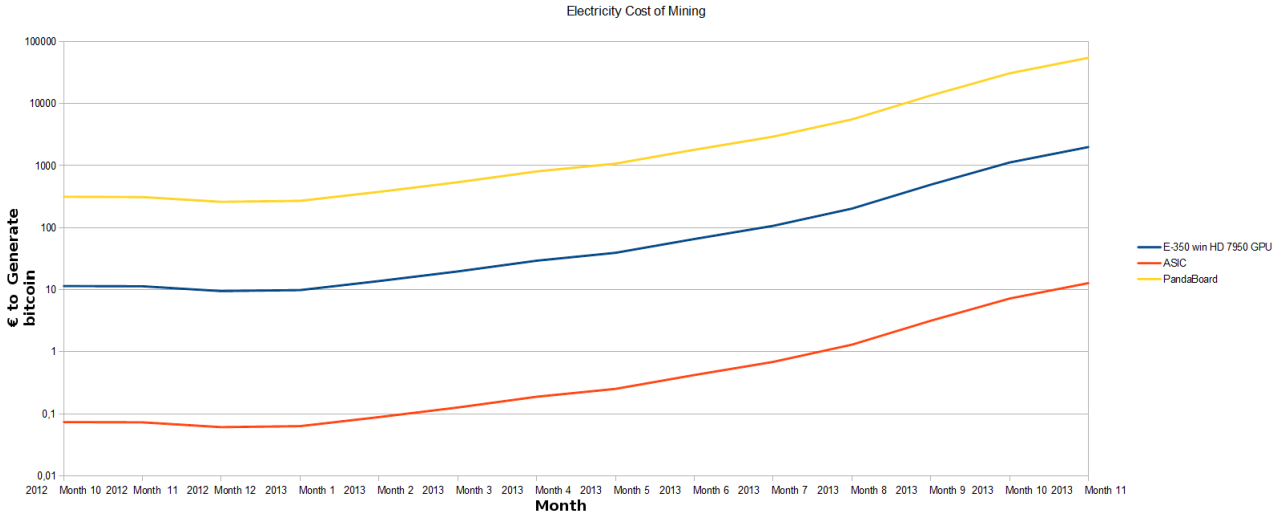

Figure 6.8: Logarithmic diagram showing cost of electricity for mining a bitcoin in a given month

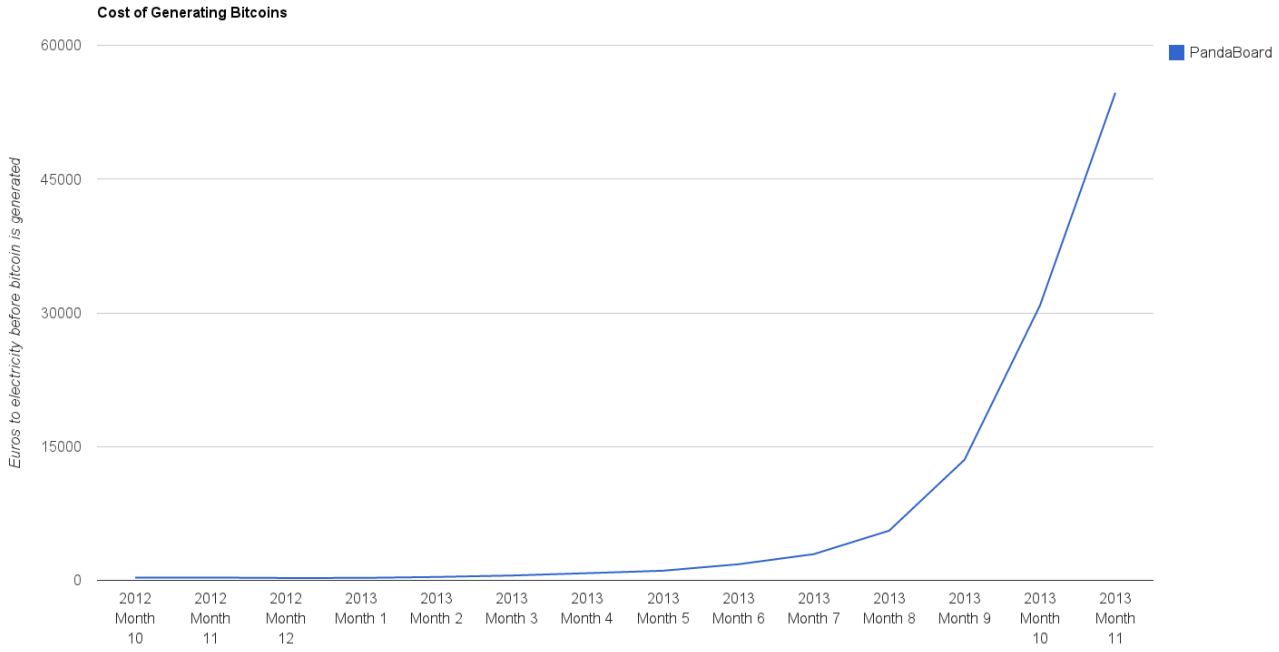

Figure 6.9: Cost of electricity in euros to generate bitcoin in given month

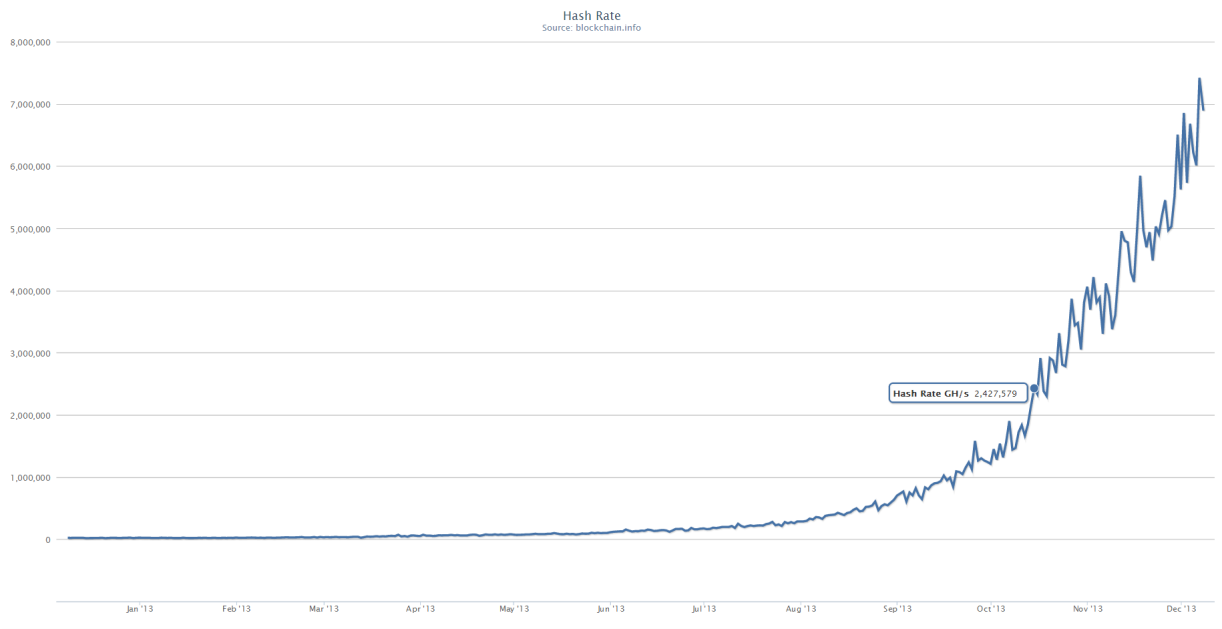

Figure 6.10: Network's Hashrate

6.3.4 Profit Diagrams

In this section, we continue with some diagrams that illustrate the costs of mining, and also try to show how much profit these devices should make on the average. Bitcoin exchange values follow the values of the Bitstamp's graph shown in Figure 6.11 [6]. The graph's values are in dollars and are converted to euros with an exchange rate of 1.35 dollars to the Euro.

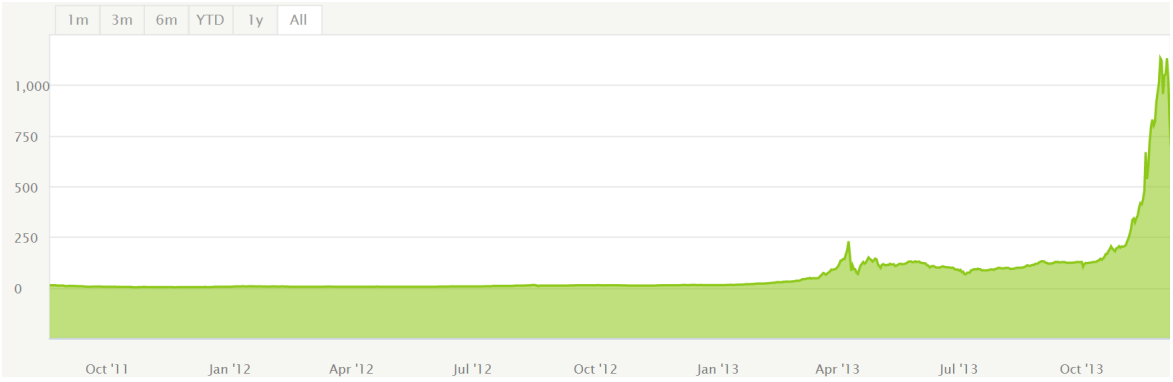

Figure 6.11: Bitcoins value in dollars graph from Bitstamp

[6] Bitstamp 8.12.2013 `https://www.bitstamp.net/`

In order to calculate income when electricity costs are deducted, we need to calculate the monthly generating time of bitcoin. We do this by dividing hashrate of the network with devices own hashrate, then resulting value is multiplied by 10, which is the average time in minutes to generate a block. Then we divide previous result with 60, 24 and 30 to obtain how many months in average it takes to find a block. To convert this to bitcoins, we need to divide previous result with 25, which was the number of bitcoins given by each block at the time.

$$\frac{\frac{NHashrate \times 10}{OHashrate}}{60 \times 24 \times 30 \times 25} \tag{6.2}$$

The income rate per month can be calculated based on formula 6.2 by raising it to the power of -1. The monthly electricity requirement for each device is calculated similarly to the formula 6.1, from where we get devices electrcity cost by bitcoin as shown in figure 6.7. The main difference is that the network hash rate changes monthly, unlike as shown in Figure 6.7. These formulas and knowlage of device and network hashrate allows us to deduct the electricity cost from the income as shown in Figure 6.12, where also the monthly bitcoin value is taken into account.

	E-350 win HD 7950 GPU	ASIC	Pandaboard
October 2012	-6.82	1,097.39	-0.74
November 2012	-6.66	1,108.03	-0.74
December 2012	0.24	1,568.26	-0.73
January 2013	1.13	1,627.78	-0.73
February 2013	10.48	2,251.18	-0.72
March 2013	17.87	2,743.46	-0.71
April 2013	20.22	2,900.10	-0.70
May 2013	24.12	3,160.64	-0.70
June 2013	2.93	1,747.77	-0.72
July 2013	-8.54	982.78	-0.74
August 2013	-15.07	547.56	-0.75
September 2013	-19.01	285.10	-0.75
October 2013	-21.25	136.00	-0.75
November 2013 First half	-18.78	300.68	-0.75
November 2013 second half	-13.60	645.62	-0.74

Figure 6.12: Income

The figure 6.12 shows the extent to which GPU mining is at or close to break-even point. The value is increasing constantly and it is very likely that the people who are mining will not sell their bitcoins as they generate them.

It is a deflating currency and, therefore, in theory, profits should increase over time. For example, if someone mined bitcoins with a GPU with a value of 11 dollars for bitcoin in 2012 November and generated a loss of 6.82 euros as described in Figure 6.12, the miner would have profited by selling those bitcoins a year later when the bitcoin's value had risen to over 1130 dollars. This increase in price is shown clearly in figure 6.13 as the ASIC miners hash rate remains the same although the highest profit is still reached during May 2013. Reason for this is that the network hash rate was not so high as prior to May 2013, but the value of bitcoin had already risen. Later the hash rate increase was not covered by the bitcoins increased value. it should be noted that income values in figure 6.12 and 6.13 are not profits because they should also include the device and labour costs. Figure 6.13 is a graphical representation of the data shown in Figure 6.12 to illustrate the different income figures after the electricity cost has been deducted from income.

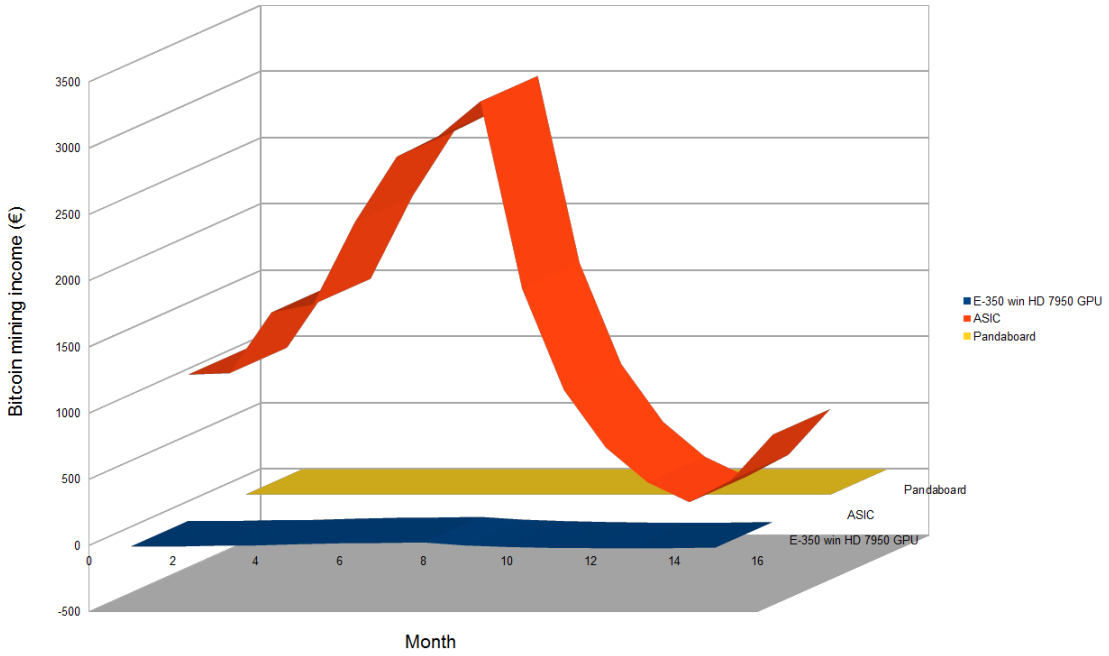

Figure 6.13: Income according to 0.15euros/kWh electricity bill using ASIC, E-350 with 7950 and Pandaboard Months correspond to Figure 6.12 Months

Chapter 7

Discussion

7.1 Further Thoughts

Efficiency requirements to mine profitability changes frequently, which means that the calculated earnings for these devices will not apply to current hash rates. We assume that the hash rate will continue to rise. The exchange value of bitcoins presumably rises in the long term, but is less predictable than stock shares. As mentioned in section 6.3.3, GPU mining will become unprofitable soon and tables in Figures 6.12 already suggest that this is the case. ASIC miners are over hundred times more efficient, and it is doubtful whether the GPU chip is capable of turning a profit out of Bitcoin mining anymore.

Other cryptocurrencies have appreared too. One is litecoin, which seems to be based on the same basic concept as Bitcoin, but transaction checks appear to be more frequent and it uses scrypt algorithm. Scrypt consumes more memory than bitcoin algorithm, thus making dedicated miners more expensive to build. Dedicated Bitcoin miners are relatively cheap to manufacture and are sold for 150 - 250 dollars, which is less than a high-end graphic card.However, a dedicated miner cannot be used for anything else. On the other hand, no reason exists why litecoin should not have dedicated miners, which seems to one of the main goals of the currency. It seems litecoin generates blocks every 2.5 minutes on the average, four times faster than Bitcoin's rate, so it might be more suitable for, e.g., fast micropayments.

Arguably, a 2.5 minute transaction verification time would have undoubtedly been better suited for some types transactions. On the other hand, specialized mining devices in Bitcoin generate less profit for the botnets because a relatively few people have these kind of miners and this makes them difficult targets for botnets, while traditional PCs do not generate enough

bitcoins to make it worthwhile taking a risk. From this viewpoint, when the botnet operators begin to realize that they will be able to actually generate more profit from litecoin, there could be a noticeable rise in litecoin and other scrypt based crypto-currency networks.

Bitcoin has a 10 minute verification time because network balances difficulty in a manner that on the average group of transactions is accepted in block chain and thus considered valid. For this reason, is doubtful that Bitcoin could ever fully replace fiat currencies. However, Bitcoin has a chance of being a currency for Internet purchases. In our view, a need exists for an easy-to-use crypto-currency that would become the new Internet currency. Some opponents say, however, that one of the challenges Bitcoin has to overcome appears to be whether it should be regarded as property or currency, especially in the US, where competing currencies are illegal. Bitcoin is becoming a well-known currency, and easy ways to purchase bitcoins from Bitcoin ATM machines [6] already exists.

An aspect that seems troubling for Bitcoin is that the transaction ledger or block chain, which is stored in every Bitcoin node, is becoming larger. In January 2013 the block chain consumed around 4GB, but three months later, at the beginning of April it, already exceeded 6GB. By October 2013, it had passed the 10GB mark. It was not a dramatic growth, but it is unclear how large it would become if Bitcoin became "the money of the future". Not even the first Internet protocols were perfect, moreover, and storing a huge ledger might not actually be a major problem, even in mobile devices as many phones are already capable of storing 32GB. Having said that, Bitcoin is still a new currency with a relatively small user base.

How much storage space each transaction needs on average? Comparing this with transactions made by Bitcoin's competitors such as Visa and Paypal would be an interesting question to study. An approach could involve estimation of monthly transactions handled by one of the bitcoin competitor and multiply that with an average transaction storage requirement and further estimate if storage requirement for block chain ledger would increase faster than storage capacity technology allows it to grow.

Unofficial Bitcoin clients exists as descried in section 3.1. Let us say, for example, someone develops an unofficial Bitcoin wallet client that gains traction from users. If this kind of client could acquire more than 60% of all wallet users, would the developer of such a client be able to alter Bitcoin network rules, or does bitcoin have some hidden mechanism to prevent this? Users could change their wallet client if they do not agree with the developer's decision. However, bitcoin network might already have problems with malicious rules before anything could be done to prevent it. In this case, the currency would divide into two different currencies although it is unclear

how message filtering would affect each network.

First and foremost, bitcoin might seem a currency that protects privacy. Unfortunately, this is not the case. Wallet users can, however, create new account for each transaction they receive to hide as much of their previous transactions as possible. As explained earlier in senction 2.1, Bitcoin transactions are chained and paying from multiple accounts reveal all user's accounts used in transaction payment. Because transactions are public, anyone who knows someone's Bitcoin address will be able to analyse the histories of these accounts. This analysis could reveal the user's transaction history and current account balance. In Bitcoin, money transfers are public, and it is the user's own job to keep him or herself hidden. This can be accomplished by making new bitcoin address each time user receives bitcoin or by using bitcoin laundry services.

An analysis can also reveal multiple accounts that the user owns. As an example, if the user pays for something that exceeds the balance of one account, then the other account balance has to be used. The input field of transaction reveals the accounts used for transactions.

"Silk Road is dead" article that argues if Silk Road had used cash, it would have actually been more difficult to stop [1]. Money laundering services naturally exists, but another Wired article claims that this bitcoin money laundering does not work well [2]. The reason for this is that not enough transactions exists to effectively hide from prying eyes. This is even more true when trying to hide large amounts of bitcoins.

The "Structure and Anonymity of Bitcoin" paper includes an analysis of bitcoin users. To quote the article, "users started to maintain their bitcoin balance, so the percentage of dormant coins has again increased to a now almost steady value of around 60 percent (given a cut off of three months)" [17]. The statement from the paper, however, does not mean that as much as 60% of bitcoins are forgotten, but this could become a potential problem for Bitcoin in future. Nobody claims these coins, but they just exist in accounts that nobody uses. Perhaps Bitcoin should have included some mechanism that would redistribute the "lost" bitcoins as a block reward in the event of the money being unused for a long time. For example If, the Bitcoin wallet had not been opened in 20 years, it could be argued that these bitcoins are lost. From this viewpoint, all the near intended 21 million bitcoins will not be seen in circulation as some of them will be lost in one way or another.

The lesson to be learned from all this is that people are extraordinarily

[1] Robert Mcmillan, Wired, 10.04.13 `http://www.wired.com/wiredenterprise/2013/10/silk_road/`

[2] Robert Mcmillan, Wired, 27.8.2013 `http://www.wired.com/2013/08/bitocoin_anonymity/`

resourceful when money is involved. Article from Extremetech [3] argues that the Bitcoin network performance outperforms the combined performance of the top 500 supercomputers. When something is profitable, someone will eventually take the bait and try to optimize it as much as possible to gain as much profit as possible. With bitcoin, the ASIC devices are a good example. They are drastically more efficient than general purpose systems. If a similar peer-to-peer ecosystem were to be introduced for medical purposes, for example to solve another type of problem that required large amount of computing power, it might experience a success in a distributed computing environment similar to the Bitcoin. if these machines were at homes, there would not be the need for such excessive cooling as supercomputers require either. In some cases, it might even replace the electricity heaters in homes. From projects point of view, maintenance requirement should decrease, and the fees and costs should be much more predictable. As stated in a datacenter CFD modeling study, to save power through a high ambient datacenter operation, In a typical datacenter, almost 40% of the total power consumption is spent on data center cooling [1]. When these machines are at homes, there would be less heat lost compared to district heating used by data centers because heat is generated in house and no transfer is required.

7.2 On The Future of Bitcoin

The first impression from the mainstream media was that bitcoins are used on drug transactions in the Silk Road marketplace [7] and other unlawful practices. Now that the founder of Silk road has been arrested, it seems that Silk road is no longer the driving force behind Bitcoin, if it ever was. On the day that the founder of Silk Road was arrested, the value of bitcoins took a deep dive of over 30 percent [4], [5] . Fortunately, for bitcoin owners, the value of bitcoins climbed back to its previous value just a few days after the incident, which may allow bitcoins to be seen in a more positive light than earlier.

Already, Bitcoin has started to receive more attention and new Bitcoin ATM machines are being introduced. One of them is going to be placed in Finland and it seems that Baidu is starting to adopt bitcoin payments

[3] Grant Brunner, ExtremeTech, 13.4.2013 http://www.extremetech.com/extreme/155636-the-bitcoin-network-outperforms-the-top-500-supercomputers-combined

[4] Henry Blade, Bittiraha.fi, 6.9.2013 https://bittiraha.fi/content/silk-roadin-kaatuminen-toi-bitcoinille-median%C3%A4kyvyytt%C3%A4

[5] Robert Mcmillan Roberts, Wired, 10.04.13 http://www.wired.com/wiredenterprise/2013/10/silk_road/

according to some news in bittiraha.fi [6]. Unfortunately no major players that would generate a greater interest in bitcoins. There are, however, a few things casting a shadow over Bitcoin's future. A few of them are technical such as the fact that the merchants and buyer have to wait over 10 minutes to be sure that the payment has actually occurred. This is not such a problem for internet stores such as Amazon, since the nature of their business does not require hasty transactions. Amazon, however, has decided to launch a currency of their own and ignore bitcoin for now.

Bitcoin has also been considered an opportunity for smaller businesses. A Wall Street article published last year, states, "Others note that credit-card swipe fees can be as high as 3% of sales, while Bitcoin services typically charge less than 1%. And, they say, Bitcoin transactions are final, unlike credit-card charges, which can be disputed. A merchant using Bitcoin can decide whether to issue a refund, though this could be a turn off for some customers".[30]

Fluctuating market value is also a problem for seller in addition to technical issues such as a 10 minute average processing time. Even after waiting waiting 10 minutes, bitcoin network might dismiss or make block orphan if different block branch is later chosen. For traditional stores, restaurants, and particularly fast food restaurant, a 10 minute waiting time makes the whole process impossible to cope with. Also, legal issues create additional work. For company, it would also be difficulty to fill in tax reports about a fluctuating currency, which is still not viewed as a real currency. 3rd party company could do the exchange to traditional currency, but it would mean, in reality, that company has outsourced bitcoin handling.

Some solutions have been proposed and are being used to eliminate the 10 minute waiting time. One of them is called fast transactions, but unfortunately this seem to allow double spending schemes [20]. Because bitcoins cannot be duplicated, one of the double double spending transactions fails. In double-spending, one way to double spend is to create two transactions. One to the targeted merchant and one to the buyer's other Bitcoin account. In this case, a 50/50 chance exists of a miner choosing the buyer's transaction over the seller's transaction. Bitcoin network has an artificial restriction dictating that there can be only one transaction per each user in every block. If the buyer's account had fewer bitcoins than both of the transactions are worth and no bitcoins are deposited into the buyer's account, later transaction will fail. Bitcoins were not designed to handle fast transactions, and merchants take the risk that they might not be aware of with fast transaction.

[6]Outi Huotari,Bittiraha.fi 15.9.13 `https://bittiraha.fi/content/viikkokatsaus-5-kiinan-google-tarjoaa-palvelua-bitcoineja-vastaan`

Bitcoin could have better documentation for the merchants. Bitcoin Wiki does offers decent general information on Bitcoin, but lacks details and at least some kind of structure. The documentation should be something that is detailed enough for someone to develop their own Bitcoin client and also structured so that it has a clear hierarchy, similarly as in, e.g., javadocs. This would allow merchants to develop a more integrated Bitcoin implementation. Multiple ready-to-use implementations exists for accepting payments in bitcoins, but realistically these are not something that, e.g., Valve would use in their Steam service. Assumably many larger companies would want to create their own, and it is difficult to see just how much effort it would require to implement more integrated Bitcoin payment system. Smaller companies might be happy with 3rd party APIs such as one offered by Blockchain.info [7].

Currently, transactions with very low rewards have difficulties being processed. The value of bitcoin has risen during 2013 more than many other investments, but it is unclear if Bitcoin is going to be a cheaper alternative to Visa or Paypal once the transactions reward share rises. bitcoin will balance its value based on demand. Similarly, bitcoin adjusts its computing resources by making less efficient devices unprofitable. This will either encourage or discourage miners to mine and thus at least tries to ensure there will be efficient miners as long as a demand exists for bitcoins. However, if current gap of transactions per block is not removed, transaction rewards might be adjusted based on demand, which might make bitcoin less attractive compared to, e.g., Paypal. Someone might question if this artificial block size rule is already restricting bitcoins growth.

[7]Blockchain API. 1.2.2014 `http://blockchain.info/api/blockchain_wallet_api`

Chapter 8

Conclusion

Bitcoin is complex currency system that exists in a legally grey area of the law. This thesis gives some background information on Bitcoin and provides a basics of Bitcoin, explaines how it is structured, the nature of its transactions, blocks, the block chain and so on.

Two different types of mining, solo and pooled, were introduced. Solo mining resembles unpredictable gambling to some extent, while pooled mining implies a steadier revenue flow without big surprises. Bitcoin clients are either web-based or local-software-based ones. Both have their own strong and weak points. Web-based clients require trust from the users, whereas locally installed software clients are slow and more expensive for the user.

For mining profitability, we conclude that it is best to acquire a mining device with the highest possible computational efficiency because that is the key to profit from Bitcoin mining. We estimated from pool data that over 30 percent of miners were generating loss rather than making a profit. Currently, the most efficient devices are ASIC miners, but we estimated that a large group of users are still using CPU for inefficient mining. A large energy efficiency gap exists between CPU and the GPU, and an even larger gap exists between GPU and ASIC miners.

Miners are currently, and most likely in the future, mining most profits from dedicated mining equipment. Other devices will either generate loss or very small profit.

Miners collect network and transaction rewards by gathering transactions into blocks and generating the proof of work that at the same time accepts block of Bitcoin users transactions. Bitcoin is a complex monetary ecosystem that tries to create interest in the currency, and at the same time, pays mining community for keeping the integrity of Bitcoin intact.

Finally, from an environmental and a profitability perspective, it can be concluded that energy efficiency is difficult to compare. It is easy to state that

Bitcoin uses an amount of electricity that is equivalent to 31 000 households, but ignore a comparison to similar services. Bitcoin would allow people to use money without the intermediary banks, which means that a truly fair comparison should be done in terms of the electricity needs of Visa and the wider banking industry.

Chapter 9

Future Work

Bitcoin has started to receive interest in the research community in these last few years. Prior to 2012, not enough research to comfortably write a background study for a master's thesis on Bitcoin. More recently, more articles and research have emerged, but still many areas are not covered yet. Bitcoin protocol is one of them. The earlier research seems to focus more on security and privacy and less on propagation and peer discovery.

We did not find any security papers describing the role of developers in Bitcoin. Bitcoin documentation claims there is "no central authority", but maybe developers act as one. They do not seem to be able to dictate the rules, but, in fact, the rules they code into their software are used to filter transactions and blocks in the Bitcoin network. This could be one of the possible research topics of the future.

As mentioned in chapter 7, a comparison of Bitcoin, Visa and Paypal would make an interesting article. Unfortunately, data for this kind of study would be difficult to acquire.

Research papers on importing Bitcoin into existing payment systems or papers from a commercial or business perspective are missing. It would be very interesting to know the thoughts of merchants who have implemented Bitcoin as part of their payment process system; what problems bitcoin has introduced and if it brought new customers, for example.

Bibliography

[1] Ahuja, N. Datacenter power savings through high ambient datacenter operation: Cfd modeling study. In *Semiconductor Thermal Measurement and Management Symposium (SEMI-THERM), 2012 28th Annual IEEE* (2012), pp. 104–107.

[2] Babaioff, M., Dobzinski, S., Oren, S., and Zohar, A. On bitcoin and red balloons. *SIGecom Exch. 10*, 3 (Dec. 2011), 5–9.

[3] Bogliolo, A., Polidori, P., Aldini, A., Moreira, W., Mendes, P., Yildiz, M., Ballester, C., and Seigneur, J. . Virtual currency and reputation-based cooperation incentives in user-centric networks. In *IWCMC 2012 - 8th International Wireless Communications and Mobile Computing Conference* (2012), pp. 895–900.

[4] Brezo, F., and Bringas, P. Issues and risks associated with cryptocurrencies such as bitcoin. ISBN: 978-1-61208-228-8, 7 2012.

[5] Bronleewe, D. A. Bitcoin nfc. Master's thesis, The University of Texas, 8 2011. urlhttp://repositories.lib.utexas.edu/bitstream/handle/2152/ETD-UT-2011-08-4150/BRONLEEWE-MASTERS-REPORT.pdf?sequence=1.

[6] Cellan-Jones, R. Bitcoin atm, 7 2013. Youtube Available: `https://www.youtube.com/watch?v=5GnJMEOPQYY#t=15`.

[7] Christin, N. Traveling the silk road: a measurement analysis of a large anonymous online marketplace. In *Proceedings of the 22nd international conference on World Wide Web* (Republic and Canton of Geneva, Switzerland, 2013), WWW '13, International World Wide Web Conferences Steering Committee, pp. 213–224.

[8] Davis, J. The crypto-currency, Oct 10 2011. Copyright - (Originally published in The New Yorker. Compilation copyright (c) 2011 The

Conde Nast Publications, Inc. All Rights Reserved.; People - Nakamoto, Satoshi; Last updated - 2011-11-02.

[9] Decker, C., and Wattenhofer, R. Information propagation in the bitcoin network. In *Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on* (Sept 2013), pp. 1–10.

[10] Dimitriou, T., and Karame, G. Privacy-friendly tasking and trading of energy in smart grids. In *Proceedings of the 28th Annual ACM Symposium on Applied Computing* (New York, NY, USA, 2013), SAC '13, ACM, pp. 652–659.

[11] Douglas Comer, Lee Dryburgh, J. H. F. H. J. K. K. W. R. C. K. R. P., and Speciner, M. Introduction to data communications and computer networks, 2006. pages 332-343, Complied by Sanna Liimatainen, Timo Kiravuo, Antti Ylä-Jääski.

[12] Ducklin, P. Anatomy of a problem - bitcoin loses 25% in value due to a long-missed bug, 3 2013. Nakedsecurity Available: http://nakedsecurity.sophos.com/2013/03/13/anatomy-of-a-problem-bitcoin-loses-25-percent-in-value/.

[13] Ferguson, N. *The Ascent of money A Financial History of the World*. Penguin Books, 2009, p. 50. ISSN:978-0-141-03548-2.

[14] Hruska, J. Amd destroys nvidia at bitcoin mining, can the gap ever be bridged?, 4 2013. ExtremeTech Available: http://www.extremetech.com/computing/153467-amd-destroys-nvidia-bitcoin-mining.

[15] Ian Traynor, Josephine Moulds, M. E., and Amos, H. Cyprus bailout deal with eu closes bank and seizes large deposits. theguardian.com, 3 2013. http://www.theguardian.com/world/2013/mar/25/cyprus-bailout-deal-eu-closes-bank.

[16] Jacobs, E. Journal of internet banking and commerce. *Journal of Internet Banking and Commerce 16*, 2 (8 2011), 201–213. Can be obtained from http://www.arraydev.com/commerce/jibc/2011-08/20110704%20JIBC%20Edwin%20JACOBS%20BITCOIN.pdf.

[17] JMicha Ober, S. K., and Hamacher, K. Structure and anonymity of the bitcoin transaction graph. *future internet* (5 2013), 237 – 250. ISSN 1999-5903.

[18] Joshua A. Kroll, I. C. D., and University, E. W. F. P. The economics of bitcoin mining, or bitcoin in the presence of adversaries. Princeton University http://www.weis2013.econinfosec.org/papers/KrollDaveyFeltenWEIS2013.pdf, 7 2013.

[19] Kaminsky, D. Let's cut through the bitcoin hype: A hacker-entrepreneur's take, 3 2013. Wired Available: http://www.wired.com/opinion/2013/05/lets-cut-through-the-bitcoin-hype/.

[20] Karame, G. O., Androulaki, E., and Capkun, S. Double-spending fast payments in bitcoin. In *Proceedings of the 2012 ACM conference on Computer and communications security* (New York, NY, USA, 2012), CCS '12, ACM, pp. 906–917.

[21] Lassi A. Liikkanen, T. N. Comparison of end user electric power meters for accuracy. Tech. rep., HELSINKI INSTITUTE FOR INFORMATION TECHNOLOGY, PO Box 9800, 02015 TKK, Finland, 6 2009. http://www.hiit.fi/files/admin/publications/Technical_Reports/hiit-tr-2009-1.pdf, ISSN 1458-9478.

[22] Lee, T. B. Feds shut down payment network liberty reserve. is bitcoin next?, 5 2013. The Washington Post Available: http://www.washingtonpost.com/blogs/wonkblog/wp/2013/05/28/feds-shut-down-payment-network-liberty-reserve-is-bitcoin-next/.

[23] Mangu-Ward, K. The bitcoin atm. *Reason 44*, 3 (2013), 72.

[24] Martins, S., and Yang, Y. Introduction to bitcoins: a pseudo-anonymous electronic currency system. In *Proceedings of the 2011 Conference of the Center for Advanced Studies on Collaborative Research* (Riverton, NJ, USA, 2011), CASCON '11, IBM Corp., pp. 349–350.

[25] Merkle, R. C. Method of providing digital signatures, 1 1982. US Patent US 4309569 A 05 01 1982 Available: http://www.google.com/patents/US4309569.

[26] Miers, I., Garman, C., Green, M., and Rubin, A. D. Zerocoin: Anonymous distributed e-cash from bitcoin. In *Security and Privacy (SP), 2013 IEEE Symposium on* (2013), pp. 397–411.

[27] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. Avaiable at http://bitcoin.org/bitcoin.pdf, 2007.

[28] Neagle, C. 10 scary facts about bitcoin. *Network World (Online)* (Jun 07 2013). Copyright - Copyright 2013 Network World, Inc. All Rights Reserved; People - Shamir, Adi; Dorit, Ron; Eichenwald, Kurt; Last updated - 2013-06-10; SubjectsTermNotLitGenreText - Shamir, Adi; Dorit, Ron; Eichenwald, Kurt.

[29] Neagle, C. Bitcoin isn't prism-proof. *Network World (Online)* (Jun 12 2013). Copyright - Copyright 2013 Network World, Inc. All Rights Reserved; Last updated - 2013-06-17.

[30] Needleman, S. More small businesses embrace bitcoin; some owners pin hopes on virtual currency, but it comes with risks. *Wall Street Journal (Online)* (6 2013). ProQuest document ID 1371585675, A version of this article appeared June 27, 2013, on page B4 in the U.S. edition of The Wall Street Journal, with the headline: Banking on Bitcoin's Novelty.

[31] of Investigation Cyber Intelligence Section, F. B., and Section, C. I. Bitcoin virtual currency: Intelligence unique features present distinct challenges for deterring illicit activity. leaked available at : `http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf`, 4 2012.

[32] Peck, M. The cryptoanarchists' answer to cash. *Spectrum, IEEE 49*, 6 (2012), 50–56.

[33] Plafke, J. Bitcoin isn't illegal because it isn't real money, 4 2013. ExtremeTech Available: `http://www.extremetech.com/internet/152349-bitcoin-isnt-illegal-because-it-isnt-real-money`.

[34] Plohmann, D., and Gerhards-Padilla, E. Case study of the miner botnet. In *Cyber Conflict (CYCON), 2012 4th International Conference on* (2012), pp. 1–16.

[35] Rankin, K. Hack and /: password cracking with gpus, part i: the setup. *Linux J. 2012*, 213 (Jan. 2012). available at:`http://www.linuxjournal.com/content/hack-and-password-cracking-gpus-part-i-setup`.

[36] Rankin, K. Hack and /: password cracking with gpus, part ii: get cracking. *Linux J. 2012*, 214 (Feb. 2012). available at:`http://www.linuxjournal.com/content/hack-and-password-cracking-gpus-part-ii-get-cracking`.

[37] Rosenfeld, M. The economics of bitcoin mining, or bitcoin in the presence of adversaries. Avaiable at `https://bitcoil.co.il/pool_analysis.pdf`, 11 2011.

[38] Ryder, G. All about bitcoin mining: Road to riches or fool's gold?, 6 2013. Tomshardware Available: `http://www.tomshardware.com/reviews/bitcoin-mining-make-money,3514.html`.

[39] Sarah Meiklejohn, Marjori Pomarole, G. J. K. L. D. M. G. M. V. S. S. A fistful of bitcoins: Characterizing payments among men with no names. University of California, San Diego George Mason University available at: `http://conferences.sigcomm.org/imc/2013/papers/imc182-meiklejohnA.pdf`.

[40] Simon Barber, Xavier Boyen, E. S., and Uzun, E. Bitter to better — how to make bitcoin a better currency. In *Financial Cryptography and Data Security* (2012), J. H. Gerhard Goos and J. van Leeuwen, Eds., 7397, p. 399.

[41] SuroWiecki, J. A brief history of money. *Spectrum, IEEE 49*, 6 (5 2012), 44 – 79. DOI: 10.1109/MSPEC.2012.6203967, ISSN:0018-9235.